ADRIAN HAASE

Computerkriminalität im Europäischen Strafrecht

Internet und Gesellschaft
9

Mohr Siebeck

Internet und Gesellschaft

Schriften des Alexander von Humboldt Institut
für Internet und Gesellschaft

Herausgegeben von
Jeanette Hofmann, Ingolf Pernice,
Thomas Schildhauer und Wolfgang Schulz

9



Adrian Haase

Computerkriminalität im Europäischen Strafrecht

Kompetenzverteilung, Harmonisierungen und Kooperationsperspektiven

Mohr Siebeck

Adrian Haase, geboren 1986; Studium der Rechtswissenschaft an der Bucerius Law School und der Universiteit Stellenbosch (Südafrika); Kollegiat im Kompetenznetzwerk für das Recht der zivilen Sicherheit in Europa (KORSE) des Bundesministeriums für Bildung und Forschung und wiss. Mitarbeiter am Alexander von Humboldt Institut für Internet und Gesellschaft, Berlin; 2015 Gastforscher an der Università degli Studi di Parma (Italien) und 2016 an der Harvard Law School (USA); 2017 Promotion; seit 2014 Rechtsanwalt, Berlin.

e-ISBN PDF 978-3-16-155406-3
ISBN 978-3-16-155406-3
ISSN 2199-0344 (Internet und Gesellschaft)

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliographie; detaillierte bibliographische Daten sind im Internet über *http://dnb.dnb.de* abrufbar.

Das Buch wurde von Gulde Druck in Tübingen gesetzt, auf alterungsbeständiges Werkdruckpapier gedruckt und von der Buchbinderei Spinner in Ottersweier gebunden.

Vorwort

Die vorliegende Arbeit wurde im August 2016 von der Juristischen Fakultät der Humboldt-Universität zu Berlin als Dissertation angenommen. Bis zu diesem Zeitpunkt publizierte Literatur und Rechtsprechung sind umfassend verarbeitet. Für die Drucklegung sind bis einschließlich Juli 2017 erschienene Publikationen ergänzend aufgenommen worden.

Der erfolgreiche Abschluss eines solch herausfordernden Projekts wäre ohne die durchgängige Unterstützung vieler Personen nicht möglich gewesen. Zuvorderst ist an dieser Stelle mein Doktorvater Herr Professor Dr. Bernd Heinrich zu nennen. Seine vertrauensvolle, motivierende und auch kritische Begleitung meines Forschungsvorhabens verdient meinen besonderen Dank!

Herrn Professor Dr. Martin Heger danke ich für die zügige Erstellung des Zweitgutachtens.

Darüber hinaus bedanke ich mich bei Herrn Professor Dr. Dr. h.c. Ingolf Pernice, Frau Dr. Karina Preiß und allen anderen Kolleginnen und Kollegen am Alexander von Humboldt Institut für Internet und Gesellschaft (Berlin) für die Schaffung eines inspirierenden Forschungsumfelds mit vielen akademischen Freiräumen für eigene Projekte. Für die Aufnahme ins Kompetenznetzwerk für das Recht der zivilen Sicherheit in Europa (KORSE) sowie die großzügige finanzielle und ideelle Förderung meines Forschungsprojekts danke ich dem Bundesministerium für Bildung und Forschung.

Außerdem bedanke ich mich ganz herzlich bei Herrn Professor Dr. Stefano Maffei von der Juristischen Fakultät der Universität Parma (Italien) und Herrn Professor Dr. Urs Gasser vom Berkman Klein Center for Internet and Society der Harvard Law School (Cambridge, USA) für die Einladungen als Gastforscher und die Einbindung in deren internationale Forschergruppen. Durch viele wertvolle Gespräche über Europäisches Strafrecht und Cybersicherheitsrecht ist meine kontinentaleuropäische Sicht auf die juristische Wissenschaft ein ums andere Mal herausgefordert sowie erfolgreich um die globalen Perspektive erweitert worden.

Für zahlreiche unschätzbare Anmerkungen und Hinweise zum Exposé sowie zum Manuskript danke ich Herrn Professor Dr. Edmund Brandt, Hannfried

Leisterer, Dr. Sebastian Leuschner, Hanna Soditt sowie insbesondere Emma Peters und Andreas Haase.

Der wichtigste Dank gilt schließlich meinen Eltern Anke und Andreas, meinen Schwestern Antonia und Ariane sowie insbesondere meiner Ehefrau Maike, auf deren familiäre Unterstützung ich mich in jeder Lebensphase bedingungslos verlassen kann. Ihnen ist diese Arbeit gewidmet.

Berlin im Sommer 2017 *Adrian Haase*

Inhaltsverzeichnis

Einleitung

I. Thematische Ausgangslage

Computer und Netzwerkstrukturen bieten zahlreiche Möglichkeiten zur Erstellung, Speicherung, Vervielfältigung und Versendung von Daten. Das Vordringen von Computern, des Intranets und vor allem des Internets in nahezu sämtliche Lebensbereiche ermöglicht Kriminalitätserscheinungen, die Staat und Gesellschaft vor sich stetig erneuernde Herausforderungen stellen. Ausmaß und Schäden von Straftaten, die gegen oder mithilfe von Computer(systeme)n begangen werden, steigen von Jahr zu Jahr.[1] Die Bandbreite von Delikten, die im Zusammenhang mit Computern und Netzwerksystemen verübt werden können, ist sehr groß. Sie erfasst herkömmliche Delikte, wie Betrug und Beleidigung unter Verwendung moderner Technologien, die Verbreitung illegaler Inhalte, wie Kinderpornografie, über das Internet oder andere Netzwerkstrukturen genauso wie strafrechtlich relevante Urheberrechtsverletzungen durch Verwendung von Computer[systeme]n, aber auch Angriffe auf elektronische Netze, wie Distributed-Denial-of-Service-Angriffe (DDoS) oder Hacking.[2] Dabei haben die meisten mit Sicherheitspolitik befassten Akteure bereits die Notwendigkeit von Präventionsmaßnahmen erkannt, beispielsweise, dass die Sicherheit von computergestützten Systemen den modernen technischen Missbrauchsmöglichkeiten anzupassen ist oder dass die Nutzerinnen und Nutzer moderner Technologien für die Relevanz und Verletzlichkeit persönlicher Daten stärker zu sensibilisieren sind. Daneben bleibt das Strafrecht jedoch ein entscheidender Faktor bei der Kriminalitätsverhütung und -bekämpfung und stellt damit einen signifikanten Bestandteil des Rechts der zivilen Sicherheit dar.[3]

---

[1] Vgl. beispielsweise die Hewlett-Packard „Cost of Cyber Crime"-Studie 2015 (Global), S. 4 f.; abrufbar unter: http://www8.hp.com/de/de/software-solutions/ponemon-cyber-security-report/ (Stand: 07.08.2017).

[2] Siehe dazu KOM (2007) 267 endg.

[3] Siehe diesbezüglich: *Haase*, in: Gusy/Kugelmann/Würtenberger (Hrsg.), Zivile Sicherheit, S. 517 (518 f.).

Auf nationaler Ebene reagierte die Legislative bereits 2007 mit dem Strafrechtsänderungsgesetz zur Bekämpfung der Computerkriminalität.[4] Allerdings haben das nahezu zwangsläufige Auseinanderfallen von Begehungs- und Erfolgsort bei internetbasierten Delikten sowie grenzüberschreitende Begehungsmodalitäten auch schon in der Vergangenheit dazu geführt, dass die ergriffenen und zu ergreifenden Maßnahmen über den einzelstaatlichen Bereich hinausgehen. Daher haben sich auch internationale Institutionen des Themenbereichs angenommen. Neben Aspekten der internationalen Zusammenarbeit bei der Verbrechensbekämpfung durch Kooperationsvereinbarungen, Datenaustausche und prozessuale Erleichterungen bei der Verhinderung, Aufklärung und Verurteilung von Computerkriminalität spielt dabei die Angleichung des materiellen Strafrechts eine wesentliche Rolle. In Gang gesetzt wurde dieser Prozess durch den völkerrechtlichen Vertrag der „Budapester Konvention gegen Datennetzkriminalität“,[5] der im Oktober 2001 von den meisten Mitgliedern des Europarats sowie von den USA, Kanada, Japan und Südafrika unterzeichnet wurde. Dieser Vertrag verfolgt das Ziel, die einzelnen nationalstaatlichen Strafvorschriften einander anzugleichen, um dadurch die grenzüberschreitende Verfolgbarkeit zu effektivieren.

Im Rahmen der Europäischen Union erstrecken sich die Bemühungen vom „Rahmenbeschluss zur Bekämpfung von Betrug und Fälschung im Zusammenhang mit unbaren Zahlungsmitteln“[6] über die „Richtlinie zur Bekämpfung des sexuellen Missbrauchs und der sexuellen Ausbeutung von Kindern sowie der Kinderpornografie“[7] bis hin zu der im August 2013 verabschiedeten und im September 2015 flächendeckend umgesetzten „Richtlinie über Angriffe auf Informationssysteme“[8]. Seit dem Inkrafttreten des Vertrags von Lissabon[9] hat die Europäische Union gem. Art. 83 Abs. 1 UAbs. 2 AEUV die Kompetenz, durch Richtlinien Mindestvorschriften hinsichtlich Straftaten und Strafen im Bereich der Computerkriminalität festzulegen. Auf dieser Grundlage kann sie auch zukünftig die Harmonisierung des materiellen Strafrechts vorantreiben.

---

[4] Einundvierzigstes Strafrechtsänderungsgesetz zur Bekämpfung der Computerkriminalität (41. StrÄndG) vom 7.8.2007, BGBl. I 2007, S. 1786.

[5] Übereinkommen über Cyberkriminalität des Europarats v. 23.11.2001 (Cybercrime Convention = ETS Nr. 185), in Kraft getreten am 1.7.2004, von der Bundesrepublik unterzeichnet am 23.11.2001, ratifiziert am 9.3.2009 und in Deutschland in Kraft getreten am 1.7.2009 gem. dem Gesetz v. 5.11.2008; BGBl. II 2008, S. 1242 (1243); BGBl. II 2010, S. 218.

[6] Abl. L 149 v. 1.6.2001, S. 1; siehe unten, Kap. 3 § 9.

[7] ABl. L 335 v. 17.12.2011, S. 1; siehe unten, Kap. 3 § 10.

[8] ABl. L 218 v. 14.08.2013, S. 8; siehe unten, Kap. 3 § 11.

[9] ABl. C 306 v. 17.12.2007, S. 1.

Am 30. Juni 2009 hatte das Bundesverfassungsgericht im Rahmen seines sog. Lissabon-Urteils[10] über die Vereinbarkeit mehrerer wegweisender Änderungen im Vertragswerk der Europäischen Union durch den Vertrag von Lissabon mit dem deutschen Verfassungsrecht zu entscheiden. Insbesondere wurde geprüft, „ob Rechtsakte der europäischen Organe und Einrichtungen sich unter Wahrung des gemeinschafts- und unionsrechtlichen Subsidiaritätsprinzips in den Grenzen der ihnen im Wege der begrenzten Einzelermächtigung eingeräumten Hoheitsrechte halten“ und „ob der unantastbare Kerngehalt der Verfassungsidentität des Grundgesetzes nach Art. 23 Abs. 1 Satz 3 in Verbindung mit Art. 79 Abs. 3 GG gewahrt ist“[11]. Eine besondere Rolle in den Ausführungen des Bundesverfassungsgerichts spielen dabei die Auswirkungen der Änderungen der Europäischen Verträge auf das Strafrecht, da sich vor allem materielles Strafrecht als Grundpfeiler der „demokratischen Selbstgestaltungsfähigkeit eines Verfassungsstaates“[12] darstelle. Hinsichtlich des Art. 83 Abs. 1 AEUV kommt das Bundesverfassungsgericht letztlich zu dem Ergebnis, dass eine verfassungskonforme Auslegung möglich, aber auch nötig sei.[13] Damit liegt das höchste deutsche Gericht im Ergebnis auf einer Linie mit anderen mitgliedstaatlichen Verfassungsgerichten.[14]

Neben diesen Harmonisierungsbestrebungen hinsichtlich des materiellen Strafrechts der Mitgliedstaaten stellen Kooperationsvereinbarungen und -instrumente einen weiteren maßgeblichen Baustein der Bekämpfung der Computerkriminalität in Europa dar. Anfang 2013 wurde dazu das Europäische Zentrum zur Bekämpfung von Cyberkriminalität (European Cybercrime Center) errichtet. Dessen zentrale Aufgaben sind das Sammeln von Informationen, die Ausbildung der nationalstaatlichen Behörden und die Unterstützung bei einschlägigen Ermittlungen. Zusätzlich soll das European Cybercrime Center als zentraler Kontaktpunkt für alle mit diesem Themenfeld Befassten fungieren.[15]

Wie diese überblicksartige Darstellung zeigt, bewegen sich die mit dem Phänomen der Computerkriminalität verbundenen tatsächlichen Herausforderungen und juristischen Fragestellungen vor allem im Grenzbereich zwischen Strafrecht, Verfassungsrecht und Europarecht, was durchgängig eine Berücksichtigung intradisziplinärer Erwägungen verlangt.[16] Zentral ist dabei die Frage, wie die Com-

---

[10] BVerfGE 123, 267 ff.

[11] BVerfGE 123, 267 (339 ff.).

[12] BVerfGE 123, 267 (359).

[13] BVerfGE 123, 267 (411 f.).

[14] Siehe unten, Kap. 2 § 7 C. I. 1. b.

[15] *Gercke, M.*, ZUM 2012, 625 (628 f.).

[16] Auch *Ambos*, Internationales Strafrecht, § 9 Rn. 4 und *Hecker*, Europäisches Strafrecht, Kap. 1 Rn. 9 ff., weisen auf die Qualität des Europäischen Strafrechts als intradisziplinäre

puterkriminalität unter Beachtung der Kompetenzverteilung zwischen Europäischer Union und ihren Mitgliedstaaten sowie unter Wahrung der nationalen Verfassungsidentitäten der Mitgliedstaaten bestmöglich bekämpft werden kann.

II. Zielbestimmung der Arbeit

Die Arbeit verfolgt das Ziel, sich dem Begriff der Computerkriminalität aus Art. 83 Abs. 1 UAbs. 2 AEUV als Aspekt eines Strafrechts der Europäischen Union umfassend zu nähern:

Erstens wird nachgewiesen, dass die bisher herrschenden Definitionen der Computerkriminalität als Grundlage für europäische Strafrechtsharmonisierungen nicht genügen. Sie sind weder hinreichend bestimmt noch, vor dem Hintergrund unionsrechtlicher Interpretationsansätze, ausreichend begrenzt. Diese Kritik aufgreifend wird eine eigene Begriffsbestimmung vorgenommen, die insbesondere der neuen Qualität von Computerkriminalität als einem EU-Rechtsbegriff gerecht wird.

Zweitens werden die maßgeblichen computerstrafrechtlichen Harmonisierungsakte der Europäischen Union auf ihre Vereinbarkeit mit dem europäischen Kompetenzrecht hin untersucht. Dabei sind vor allem die gewonnenen Erkenntnisse zur begrifflichen Einordnung heranzuziehen sowie die unions- und verfassungsrechtliche Vereinbarkeit von Vorfeldkriminalisierungen als Teil eines Präventionsstrafrechts zu analysieren.

Drittens werden zukünftige Herausforderungen und Möglichkeiten, die mit der unionsrechtlichen Verankerung des Begriffs der Computerkriminalität in Art. 83 Abs. 1 UAbs. 2 AEUV verbunden sind, identifiziert. Anschließend wird über den Schwerpunkt rechtlich-normativer Entwicklungsperspektiven hinaus der aktuelle Diskussionsstand hinsichtlich einer fortschreitenden Strafrechtsintegration in der Europäischen Union aufgezeigt und einer eigenen Bewertung unterzogen.

Zusammenfassend stellt und beantwortet diese Arbeit daher im Hinblick auf den Kompetenztitel des Art. 83 Abs. 1 UAbs. 2 AEUV folgende Fragen: Was umfasst der Rechtsbegriff der Computerkriminalität? Wie nutzt die Europäische Union bisher ihre Kompetenz zur Harmonisierung der Computerkriminalität und welche unions- bzw. verfassungsrechtlichen Probleme zeigen sich? Und schließlich, welche Perspektiven bieten sich für ein zukünftiges europäisches Computerstrafrecht unter Berücksichtigung der (unions-)rechtlichen Rahmen-

---

Querschnittsmaterie hin, die zumindest zusätzliche Grundlagen im Verfassungs-, Europa- und Völkerrecht verlangt.

bedingungen sowie der beteiligten Akteure im europäischen Mehrebenensystem?

Unbestimmte Rechtsbegriffe sind im Unionsrecht zwar nicht unüblich, stellen hinsichtlich der strafrechtlichen Harmonisierungskompetenzen jedoch besondere Schwierigkeiten dar. Sowohl „Computerkriminalität" als auch „Internetkriminalität" oder gar „Cyberkriminalität" sind Begriffe, die längst nicht mehr ausschließlich in der technischen und juristischen Fachterminologie verwendet werden, sondern in den allgemeinen Sprachgebrauch Einzug gehalten und sich somit vielfach definitorisch verselbstständigt haben. Neben einer fortschreitenden Technisierung des Alltags, die unter anderem dazu führt, dass auch bei kriminellen Aktivitäten vermehrt Computer(systeme) genutzt werden und/oder diese beeinflussen und beeinträchtigen, ist die zunehmende Ausbreitung der Computerkriminalität noch auf ein anderes Phänomen zurückzuführen – auf die extensive Auslegung und Nutzung des Begriffs. Im Rahmen einer extrem weit gefassten Definition wäre es in letzter Konsequenz sogar vorstellbar, dass überhaupt nur wenige Straftaten keinen relevanten Bezug zu Computern, zum Internet oder zum Cyberraum aufweisen. Dann würde selbst eine Einigung auf einen dieser Begriffe kaum einen begrenzenden oder auch nur klärenden Effekt versprechen. Als eine zusätzliche Schwierigkeit ist anzuführen, dass die Begriffe freilich häufig nur deshalb synonym verwendet werden, um einer semantischen Eintönigkeit vorzubeugen.[17]

Für die Identifizierung eines Kriminalitätsphänomens stellt die angesprochene Begriffsweite und -ungenauigkeit noch kein nennenswertes Problem dar, solange lediglich aufgezeigt werden soll, wie groß der Anteil computer-, internet-, oder cyberbezogener Straftaten im Vergleich zur „herkömmlichen" Kriminalität ist. Bereits im Rahmen offizieller Kriminalitätsstatistiken sieht das allerdings anders aus, da diese auch der Ressourcenverteilung und (Neu-)Bewertung politischer und juristischer Schwerpunktsetzungen dienen.[18] Spätestens im rechtlich kodifizierten Bereich tauchen weitere und gravierendere Schwierigkeiten auf. Durch Art. 83 Abs. 1 UAbs. 2 AEUV ist der Kriminalitätsbereich der Computerkriminalität als harmonisierungsfähig eingeordnet worden. In diesem Bereich kann die Europäische Union mithilfe von Richtlinien Einfluss auf die nationalstaatlichen Strafrechtsordnungen nehmen. Eine begriffliche Einordnung und Eingrenzung ist daher dringend geboten.

Neben einer Begriffsbestimmung ist die Analyse und Bewertung von computerstrafrechtlichen Harmonisierungsmaßnahmen im europäischen Raum uner-

---

[17] So auch *Goodman/Brenner*, Int J Law Info Tech 2002 139 (150 f.); *Tikk/Kaska/Vihul*, Cyber Incidents, S. 101.

[18] Polizeiliche Kriminalstatistik 2014, S. 1.

lässlich. Einerseits kann so die herausgearbeitete Definition an der rechtlichen und tatsächlichen Realität gemessen werden, andererseits lassen sich dadurch Perspektiven für eine Weiterentwicklung des EU-Computerstrafrechts aufzeigen. Dazu ist insbesondere zu hinterfragen, ob Art. 83 Abs. 1 AEUV, der in dieser Form erst durch den Vertrag von Lissabon in die europäische Verträge implementiert wurde,[19] als Harmonisierungsmotor anzusehen ist. Vergleichend begutachtet wird zudem die Rolle des Europarats mit seinen völkerrechtlichen Vereinbarungen und deren Auswirkungen auf das europäische und nationale Computerstrafrecht, da dessen Vorarbeiten vielfach in die einschlägigen EU-Rechtsakte eingeflossen sind.

Ohne die Notwendigkeit von Harmonisierungsbestrebungen bezüglich des materiellen Strafrechts allgemein infrage stellen zu wollen, wird untersucht, welche Hintergründe die einzelnen Rechtsakten haben, wie sie in Literatur, Rechtsprechung und Praxis aufgenommen werden und insbesondere welche Umsetzungsverpflichtungen mit diesen Maßnahmen verbunden waren und sind. Vor allem die Einzelmaßnahmen innerhalb der Instrumente geben Aufschluss über die multifunktionalen Zielrichtungen von Abkommen, Rahmenbeschlüssen und Richtlinien. Dabei wird bezweifelt, dass die Angleichung des materiellen Strafrechts in allen betroffenen Fällen ein verhältnismäßiges Mittel zur Bekämpfung der regelmäßig grenzüberschreitenden Computerkriminalität darstellt. Während dies etwa beim Schutz kritischer Infrastrukturen vor digitalen Angriffen zutrifft, deren Auswirkungen aufgrund oftmals verbundener Informationsinfrastrukturen nicht nur national sind, dienen andere materiell-rechtliche Maßnahmen lediglich einer Vereinfachung der Verfolgbarkeit und Nachweisbarkeit durch Vorverlagerungen von Strafbarkeit, ohne allerdings dieser Strafbarkeitsausweitung äquivalent wichtige und gemeinschaftlich schützenswerte Rechtsgüter gegenüberzustellen.

Der letzte Teil der Dissertation komplettiert den hier gewählten dreigliedrigen Ansatz aus kompetenzrechtlicher Basis, strafanweisungsrechtlicher Umsetzungen und perspektivischenen Weiterentwicklungen der Computerkriminalitätsbekämpfung nach Art. 83 Abs. 1 UAbs. 2 AEUV. Die grundlegende Begriffsbestimmung einerseits sowie die Einordnung und Überprüfung der europäischen Rechtsakte als Anwendungsfälle computerstrafrechtlicher Harmonisierungen andererseits bilden damit Grundbedingungen für eine Einschätzung der zukünftigen Optionen zur Bekämpfung der Computerkriminalität im europäischen Raum der Freiheit, der Sicherheit und des Rechts. Es werden dazu

---

[19] Der Reformvertrag von Lissabon hat die „frühere Tempelarchitektur der EU“ aufgegeben; vgl. statt aller: *Hecker*, Europäisches Strafrecht, Kap. 1 Rn. 3; *Heger*, ZIS 2009, 406 (407).

verschiedene Möglichkeiten für eine verstärkte Internationalität im Computerstrafrecht aufgezeigt, die sich sowohl auf zusätzliche materielle Harmonisierungen als auch auf einen Ausbau der transnationalen Zusammenarbeit und eine Angleichung des formellen Rechts stützen und letztlich dem Ziel einer effektiveren Bekämpfung der Computerkriminalität dienen.

III. Methodische Überlegungen

Naturgemäß spielen in einer rechtswissenschaftlichen Arbeit klassische juristische Auslegungsmethoden eine maßgebliche Rolle. Insbesondere die Auseinandersetzung mit den Begrifflichkeiten „Computerkriminalität", „Internetkriminalität", „Cyberkriminalität" etc. findet unter Heranziehung der grammatischen, der systematischen, der historischen und der teleologischen Auslegung statt. Um dem vorliegenden transnational geprägten und rechtsgebietsübergreifenden Untersuchungsobjekt gerecht werden zu können, wird dieser Auslegungskanon um rechtsvergleichende sowie verfassungs-, europarechts- und völkerrechtskonforme Interpretationselemente ergänzt. Darüber hinaus ist zu beachten, dass auf Unionsebene zwar grundsätzlich die gleichen Auslegungsansätze wie im deutschen Recht verfolgt werden, eine Akzentuierung und Gewichtung der einzelnen Elemente jedoch aus genuin unionsrechtlicher Perspektive erfolgt. Die Gemeinsamkeiten und Unterschiede dieser Vorgehensweisen werden daher an geeigneter Stelle dargestellt und angewandt. Zusätzliche methodische Erweiterungen bei der Einkreisung europäischer Rechtsbegriffe werden darüber hinaus notwendig, da sich das Zusammenspiel zwischen Rechtssetzung, Rechtsanwendung und Rechtsunterworfenheit in einem europäischen Mehrebenensystem nur schwerlich ausschließlich mithilfe einer klassisch-hermeneutischen Herangehensweise abbilden lässt. Insgesamt wird durch diese methodische Vielfalt vor allem den besonderen Herausforderungen bei der Interpretation von europäischen Kompetenznormen als „Meta-Verfassungsrecht" Rechnung getragen, die sich regelmäßig nicht in einem geschlossenen Rechtssystem auslegen lassen, sondern stattdessen ein politisch und gesellschaftlich informiertes Verständnis erfordern.[20] Sichtbar wird dies beispielsweise am Dialog der verschiedenen Verfassungsgerichte in Europa bei der Rechtsauslegung im Grenzbereich zwischen Unions- und Verfassungsrecht.[21] Insbesondere für die Definition des unionsrechtlichen Computerkriminalitätsbegriffs des Art. 83 Abs. 1 UAbs. 2 AEUV bezeichnet dieser Dialog einen elementaren Baustein.

---

[20] *Hahn-Lorber*, ELJ 2010, 760 (764 ff.).

[21] *Ruggeri, A.*, in: Ruggeri, S. (Hrsg.), European Criminal Law, S. 10 (11); *von Danwitz*, in: Hatje/Müller-Graff (Hrsg.), EnzEuR Bd. 1, § 13 Rn. 34 ff.; *Voßkuhle*, NVwZ 2010, 1 (3 ff.).

IV. Gang der Darstellung

Die Dissertation gliedert sich in vier Kapitel. Im ersten Kapitel wird zunächst in die unterschiedlichen Rechtsquellen des materiellen Strafrechts und die verschiedenen Akteure bei der Strafrechtsharmonisierung eingeführt. Zusätzlich werden überblicksartig die Grundlagen und Prinzipien des Strafrechts der Europäischen Union dargestellt, soweit sie für die noch folgenden Ausführungen zur Untersuchung des Rechtsbegriffs der Computerkriminalität von Bedeutung sind. Überdies dient das erste Kapitel insbesondere der örtlichen wie sachlichen Begrenzung des analysierten Rechtsraums.

Im zweiten Kapitel folgt eine detaillierte Begriffsklärung. Ausgehend vom Begriff der Computerkriminalität[22] des Art. 83 Abs. 1 UAbs. 2 AEUV werden auch weitere relevante Begriffe wie Internetkriminalität, Cyberkriminalität, ICT-Crime etc., die häufig synonym verwendet werden,[23] definiert und voneinander abgegrenzt. Nach einer Übersicht zum aktuellen Forschungs- und Diskussionsstand anhand der rechtlichen und technischen Literatur, Rechtsprechung sowie Gesetzgebungsmaterialien wird untersucht, inwieweit der Begriff der Computerkriminalität zur Beschreibung eines harmonisierungsfähigen und -bedürftigen Kriminalitätsbereichs geeignet ist. Es zeigt sich dabei, dass sowohl der Begriff der Computerkriminalität als auch andere verwandte Begriffe unter Umständen für die Beschreibung eines Phänomens genügen, sich jedoch bezüglich eines Harmonisierungsauftrags als konkretisierungsbedürftig erweisen. Daher wird zum Abschluss des zweiten Kapitels ein neuer, restriktiverer, aussagekräftigerer und dennoch mit dem europäischen Primärrecht vereinbarer Computerkriminalitätsbegriff entwickelt und begründet.

Das dritte Kapitel behandelt schwerpunktmäßig die Rechtsakte zur Harmonisierung des europäischen Computerstrafrechts. Diese werden beschrieben, eingeordnet und anhand der im zweiten Kapitel erarbeiteten Ergebnisse bewertet, sodass schließlich über deren Vereinbarkeit mit dem EU-Kompetenzrecht entschieden werden kann. Dabei liegt ein besonderes Augenmerk auf der Zulässigkeit der Vorverlagerung der Strafbarkeit in den Vorbereitungsbereich bei einzelnen Straftaten des Computerstrafrechts unter systematischen, unionsrechtlichen und verfassungsrechtlichen Gesichtspunkten. Diese Vorfeldstrafbarkeiten

---

[22] Trotz einer Vielzahl von Arbeitsdefinitionen wird oftmals angenommen, dass eine allseits anerkannte Definition des Begriffs der Computerkriminalität bisher überhaupt nicht besteht, was die begriffliche Klärung und Eingrenzung umso relevanter macht; vgl. *Dorra*, Legislativkompetenzen, S. 209; *Fahey*, EJRR 2014, 46 (50); *Tropina*, in: dies./Callanan (Hrsg.), Self- and Co-regulation in Cybercrime, Cybersecurity and National Security, S. 5; *Watney*, JITST 2012, 61 (62).

[23] Das gilt ebenfalls für die Nutzung der englischsprachigen Begriffe *computer crime, cybercrime, high-tech crime* etc.; siehe *Clough*, Cybercrime, S. 10.

sind durch das 41. Strafrechtänderungsgesetz vom 7. August 2007 in das deutsche Strafgesetzbuch eingefügt worden und setzen Vorgaben der oben genannten Budapester Konvention des Europarats und des Rahmenbeschlusses 2005/222/JI des Rates vom 24. Februar 2005 über Angriffe auf Informationssysteme[24] um. Beispiele sind § 202c StGB, der Vorbereitungshandlungen zu den Taten nach den §§ 202a (Ausspähen von Daten) und 202b StGB (Abfangen von Daten) unter Strafe stellt, und die §§ 303a StGB (Datenveränderung) und 303b StGB (Computersabotage), die auf § 202c StGB verweisen. Wichtige Aspekte bezeichnen dabei Fragen zur Alternativlosigkeit der Umsetzung als Strafrecht, zur EU-Rechtmäßigkeit der Richtlinie 2013/40/EU und schließlich zu mitgliedstaatlichen Abweichungsmöglichkeiten.

Im abschließenden Kapitel der Dissertation werden zukünftige Entwicklungsszenarien des europäischen Computerstrafrechts aufgezeigt. Dadurch erfolgt eine Verknüpfung des zunächst umgrenzten Bereichs der Computerkriminalität mit einem übergeordneten Evolutionsprozess eines Strafrechts der Europäischen Union. Der Kriminalitätsbereich der Computerkriminalität eignet sich wie kaum ein anderer dazu, zukünftige Leitlinien einer europäischen Strafrechtssystematik und -politik darzulegen. Die Vernetzung von Computer(systeme)n und die damit verbundene Vulnerabilität von kritischen Infrastrukturen bieten Anlass, sich mit verschiedenen Entwicklungsperspektiven auseinanderzusetzen. Als denkbare Anknüpfungspunkte sind insbesondere eine Zuständigkeitserweiterung für die sich in der Errichtung befindende Europäische Staatsanwaltschaft auf den Bereich der Computerkriminalität oder eine tiefer greifende Integration des materiellen und formellen Computerstrafrechts anzuführen.

[24] Rahmenbeschluss 2005/222/JI des Rats v. 24.2.2005 über Angriffe auf Informationssysteme, ABl. L 69 v. 16.3.2005, S. 67 ff. In der Richtlinie 2013/40/EU des Europäischen Parlaments und des Rats v. 12.8.2013 über Angriffe auf Informationssysteme und zur Ersetzung des Rahmenbeschlusses 2005/222/JI des Rats, ABl. L 218 v. 14.8.2013, S. 8 ff. finden sie sich abermals.

Kapitel 1

Strafrecht als transnationale Regelungsmaterie

Nicht erst seit dem Inkrafttreten des Vertrags von Lissabon ist das jeweilige Strafrecht der Mitgliedstaaten zu einer europäischen und damit harmonisierungsfähigen Rechtsmaterie geworden. Der Kampf zwischen strafrechtlichen „Reformern" und „Traditionalisten" scheint somit erst einmal zugunsten ersterer entschieden. Kaum sind allerdings in Art. 83 Abs. 1 UAbs. 2 AEUV harmonisierungsfähige Rechtsbereiche aufgezählt, hat sich die Debatte über ein Strafrecht der Europäischen Union auf die Ebenen der Auslegungs- und Interpretationshoheiten bezüglich der Begrifflichkeiten und der zukünftigen Entwicklungsperspektiven im Spannungsfeld zwischen mitgliedstaatlicher strafrechtlicher Souveränität und den Erfordernissen einer Internationalisierung auch des materiellen Strafrechts verschoben.[1] Gegenüber der zuvor durchaus noch existenten Frage des „Ob" einer Strafrechtsharmonisierung, die durch die Kompetenznorm des Art. 83 Abs. 1 AEUV entschieden wurde, sind also die Fragen des „Wie" und des „Wie weit" in den Vordergrund der Debatte im materiellen Strafrecht der Europäischen Union getreten.

Nationales und EU-Computerstrafrecht auf der einen sowie Vor- bzw. Parallelarbeiten internationaler Institutionen wie dem Europarat und in Teilen auch der Vereinten Nationen auf der anderen Seite bedingen und beeinflussen einander. Wie zu zeigen sein wird, baut das Computerstrafrecht der Europäischen Union wesentlich auf völkerrechtlichen Konventionen auf, verfeinert jene und könnte selbstständig wiederum Vorbild für weitergehende Internationalisierungstendenzen sein. Wenngleich der Fokus dieser Arbeit maßgeblich auf dem EU-Computerstrafrecht mit seinen Begrifflichkeiten[2], Legislativakten[3] und Entwicklungsperspektiven[4] liegt, sind für ein Verständnis der Harmonisierung des materiellen Strafrechts die Einflüsse anderer Institutionen relevant.

---

[1] Exemplarisch dafür stehen die Tendenzen der Souveränitätsverteidigung in BVerfGE 123, 267 ff. einerseits und Perspektiven hinsichtlich eines Europäischen Strafgesetzbuchs andererseits; siehe etwa *Sieber*, in: GS Schlüchter (2002), S. 107 (111 ff.).

[2] Siehe unten, Kap. 2.

[3] Siehe unten, Kap. 3.

[4] Siehe unten, Kap. 4.

§ 1 Materielle Strafrechtsharmonisierung – Begriffsverständnis

Der geläufige Begriff der Harmonisierung des Strafrechts beschreibt den eigentlichen strafrechtlichen Integrations- und Koordinierungsprozess allerdings nicht umfassend. Harmonisierung bezeichnet lediglich die Angleichung von Normen. Daneben sind jedoch auch die Koordinierung (Regelungen zum prozessualen Strafrecht) und die Zusammenarbeit i. e. S. (z. B. Auslieferung und weitere Rechtshilfemechanismen) entscheidend.[5] Ebenfalls spielen die Institutionalisierung und Zentralisierung auf dem Gebiet des Strafrechts der Europäischen Union eine Rolle. Auch wenn – anders als im Völkerstrafrecht – noch keine europäische Gerichtsbarkeit besteht,[6] wurden durch Eurojust, Europol und die Ermächtigung zur Gründung einer Europäischen Staatsanwaltschaft (Art. 86 AEUV) zumindest auf exekutiver Strafverfolgungsebene europäische Institutionen geschaffen.[7]

Da das EU-Computerstrafrecht einerseits erheblich durch Vor- und Parallelarbeiten anderer internationaler Organisationen beeinflusst ist und andererseits potenziell Modellcharakter für weitere Internationalisierungen hat, soll zunächst überblicksartig auf die verschiedenen Rechtsquellen des materiellen Strafrechts und damit auf die Herkunft von Harmonisierungsbestrebungen eingegangen werden.

A. Rechtsquellen des materiellen Strafrechts

Das materielle Strafrecht speist sich aus mehreren Rechtsquellen. Zu nennen sind diesbezüglich das nationale Strafrecht, das Europäische Strafrecht, das Völkerstrafrecht und das allgemeine Völkerrecht.

I. Arten von Rechtsquellen

Grundsätzlich zu unterscheiden ist bei der Betrachtung der Rechtsquellen des materiellen Strafrechts zwischen jenen, die von Institutionen mit originärer Strafrechtsetzungskompetenz ausgehen und solchen, die lediglich als Vorschläge oder Vorgaben für eine Umsetzung durch den dazu kompetenten Gesetzgeber fungieren. Die originäre Strafrechtsetzungskompetenz bezeichnet die Befugnis, selbst Strafnormen zu erlassen, die keines weiteren Umsetzungsakts

[5] *Böse*, in: ders, (Hrsg.), EnzEuR Bd. 9, § 1 Rn. 15.
[6] Siehe unten, Kap. 4 § 14 B. II.
[7] *Böse*, in: ders. (Hrsg.), EnzEuR Bd. 9, § 1 Rn. 15; siehe dazu insbesondere unten, Kap. 4 § 14 C.

mehr bedürfen und unmittelbar die Strafbarkeit eines einzelnen Rechtsunterworfenen begründen.

Beispiel: Der Staat S erlässt ein Gesetz, das die Verbreitung von „hate speech" in Online-Netzwerken unter Strafe stellt. Daraufhin sind alle Rechtsunterworfenen unmittelbar an dieses Strafgesetz gebunden.

Demgegenüber wird regelmäßig von der sog. strafrechtlichen Anweisungskompetenz gesprochen, wenn ein Normgeber lediglich Vorgaben macht, die daraufhin erst von den strafrechtsetzungskompetenten Gesetzgebern umgesetzt werden müssen.[8]

Die Europäische Union hat die Möglichkeit, im Falle der Nichtumsetzung von Unionsrecht ein Vertragsverletzungsverfahren nach Art. 258 AEUV gegen den jeweiligen Mitgliedstaat einzuleiten. Im Europarat kommt eine Sanktionierung des Mitgliedstaats in Betracht, wenn jener seinen Vertragspflichten nicht nachkommt. Einerseits kann sein Stimmrecht suspendiert werden und andererseits steht grundsätzlich auch der Ausschluss eines Mitgliedstaats gem. Art. 8 i. V. m. Art. 3 des Statuts des Europarates zur Disposition.[9] Regelmäßig werden diese Konsequenzen jedoch aus politischen Gründen vermieden.[10]

II. Rechtsquellenübersicht und begriffliche Abgrenzungen

Für das Strafrecht besonders relevant sind europäische oder globale Rechtsquellen wie EU-Richtlinien oder völkerrechtliche Vereinbarungen.[11] Jedoch bleibt der nationale Gesetzgeber bis dato alleine kompetent zur Setzung von Strafnormen und somit Hüter des Kriminalstrafrechts. Weder völkerrechtliche Vereinbarungen noch EU-Richtlinien vermögen das jeweilige nationale Strafrecht unmittelbar zu ändern oder zu ergänzen. Eine solche formalistische Betrachtungsweise vernachlässigt jedoch europäische sowie globale Dynamiken, die bei einem Mehrebenenstrafrecht[12] mit verschiedenen Akteurskonstellationen zu beachten sind. Die Bundesrepublik Deutschland öffnet das eigene Rechtssystem beispielsweise durch die Völkerrechtsfreundlichkeit des Grund-

---

[8] *Dorra*, Legislativkompetenzen, S. 23 m. w. N.

[9] Vgl. *Reindl-Krauskopf*, ZaöRV 74 (2014), 563 (567).

[10] Weitere Hinweise zu diesem völkerrechtlichen Sanktionsmechanismus bieten *Fischer/Köck/Karollus*, Europarecht, Rn. 163.

[11] *Gercke, M./Tropina*, CRi 2009, 136 (140) m. w. N.

[12] Zu strafrechtlichen Gegebenheiten in verschiedenen Mehrebenensystemen und insbesondere zum strafrechtlichen Mehrebenensystem in der Europäischen Union siehe *Reinbacher*, Strafrecht im Mehrebenensystem, S. 365 ff.

gesetzes[13] und durch die zu jener parallel entwickelten Europarechtsfreundlichkeit[14].

Im Rahmen des Völkerrechts ist zwischen sog. *treaty (based) crimes*[15] oder auch internationalen Verbrechen[16], also den Strafnormen, die aufgrund völkerrechtlicher Vereinbarungen Eingang in die nationalen Strafrechtsordnungen gefunden haben oder finden sollen und dem klassischen Völkerstrafrecht[17] zu unterscheiden. Während erstere keinen eigenständigen Strafnormcharakter aufweisen, sondern lediglich Modell für nationale Strafnormen stehen, stellt das Völkerstrafrecht[18] selbstständige Sanktionsnormen (sog. *core crimes*[19]) auf, die durch den Internationalen Strafgerichtshof in Den Haag (IStGH) abgeurteilt

---

[13] Art. 25 S. 1 GG: „Die allgemeinen Regeln des Völkerrechtes sind Bestandteil des Bundesrechtes. Sie gehen den Gesetzen vor und erzeugen Rechte und Pflichten unmittelbar für die Bewohner des Bundesgebietes." Das BVerfG hat diesen Grundsatz in BVerfGE 112, 88 ff. konkretisiert: „Die allgemeinen Regeln des Völkerrechts sind gemäß Art. 25 GG Bestandteil des deutschen Rechts im Rang über dem einfachen Bundesrecht. Die daraus folgende Pflicht, diese Regeln zu respektieren, erfordert, dass die deutschen Staatsorgane die die Bundesrepublik Deutschland bindenden Völkerrechtsnormen befolgen und Verletzungen unterlassen, [...]".

[14] Das BVerfG hat dazu die neue Figur der Europarechtsfreundlichkeit des Grundgesetzes entwickelt. Inhaltlich stützt sich dieser Grundsatz auf die Präambel und Art. 23 GG; BVerfGE 123, 267 (346 f.).

[15] Dabei handelt es sich um die im Englischen geläufige Terminologie, um Straftaten zu beschreiben, die sich aus völkerrechtlichen Verträgen ergeben, selbst aber nicht dem klassischen Völkerstrafrecht zuzurechnen sind; vgl. *Bassiouni*, in: ders. (Hrsg.), International Criminal Law Bd. 1, S. 32 f.

[16] Der Terminus „internationale Verbrechen" ist einerseits als Oberbegriff für jedes völkerrechtliche Strafrecht, inkl. des klassischen Völkerstrafrechts, zu verstehen, bezeichnet in seiner regelmäßigen Verwendung allerdings eher Verbrechen des Terrorismus und des Betäubungsmittelhandels, da diese in den Verhandlungsmitschriften zum IStGH-Statut eine Rolle gespielt haben, jedoch nicht in den Kreis des klassischen Völkerstrafrechts aufgenommen worden sind; vgl. dazu *Robinson*, in: The Rome Statute, Chapter 11.7, S. 497 ff.

[17] Der Begriff wurde erstmalig von *Beling*, Exterritorialität, geprägt, der in diesem Beitrag die denkbare Entstehung völkerstrafrechtlicher Normen andenkt und diese als „Völkerstrafrecht" betitelt.

[18] Im deutschsprachigen Raum hat es sich in definitorischer Hinsicht durchgesetzt, unter den Begriff des Völkerstrafrechts alle Normen des Völkerrechts zu fassen, die unmittelbar eine Strafbarkeit begründen, ausschließen oder in anderer Weise regeln. Daraus ergeben sich drei notwendige Voraussetzungen, um eine Norm als völkerstrafrechtlich einzuordnen: Erstens muss sie individuell vorwerfbares Unrecht festlegen und dieses auf Rechtsfolgenseite mit Strafe bedrohen, zweitens muss sie der Völkerrechtsordnung zuzuordnen sein und drittens darf die Strafbarkeit nicht von einer Transformation der Norm in die staatlichen Rechtsordnungen abhängen; siehe dazu *Werle*, Völkerstrafrecht, Rn. 86 f. m. w. N.

[19] Vgl. zu Kernverbrechen *von Arnauld*, Völkerrecht, § 15 Rn. 1302 ff.

werden können.[20] Diese haben sich stufenweise innerhalb der internationalen Gemeinschaft entwickelt.[21]

III. Weitere Akteure bei der Computerkriminalitätsbekämpfung

Neben den genannten Institutionen und Zusammenschlüssen spielen auch weitere Organisationen im europäischen und globalen Bereich wichtige Rollen bei der Bekämpfung der Computerkriminalität. Insbesondere zu nennen sind etwa die Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (Organisation for Economic Co-operation and Development, OECD)[22], die G8-Staaten[23] und Interpol[24]. Darüber hinaus kommen teilweise auch solchen Organisationen, deren Schwerpunktbereiche abseits der Kriminalitätsbekämpfung liegen, in gewissen Überschneidungsfeldern maßgebliche Aufgaben zu, wenn Berührungspunkte zwischen Computerkriminalität und Themen wie Privatsphäre, Datenschutz oder Datensicherheit auftreten. Darunter fallen etwa die

---

[20] Völkermord (Art. 6 IStGH-Statut), Verbrechen gegen die Menschlichkeit (Art. 7 IStGH-Statut), Kriegsverbrechen (Art. 8 IStGH-Statut) und Agressionsverbrechen (Art. 8 IStGH-Statut); siehe auch *Werle*, Völkerstrafrecht, Rn. 88.

[21] Zunächst hat sich das Völkerstrafrecht durch das sog. Recht von Nürnberg (vgl. *Werle*, Völkerstrafrecht, Rn. 5), die Niederlegung im IMG-Statut (International Military Tribunal, Der Prozess gegen die Hauptkriegsverbrecher vor dem Internationalen Militärgerichtshof, S. 10–18), die Anwendung durch den Internationalen Militärgerichtshof der vier Siegermächte (International Military Tribunal, Der Prozess gegen die Hauptkriegsverbrecher vor dem Internationalen Militärgerichtshof, S. 7–9), die Bestätigung durch die Generalversammlung der Vereinten Nationen sowie die Errichtung der Ad-hoc-Strafgerichtshöfe für das ehemalige Jugoslawien und Ruanda völkergewohnheitsrechtlich verfestigt (*Werle*, Völkerstrafrecht, Rn. 5), bevor durch das Inkrafttreten des „Römischen Statuts" (IStGH-Statut; amtliche Übersetzung bei *Rosbaud*, Rome Statute of the International Criminal Court) und die damit verbundene Einrichtung des Internationalen Strafgerichtshofs in Den Haag eine Kodifikation des Völkerstrafrechts stattfand.

[22] Vor allem aus entwicklungspolitischen Erwägungen beschäftigt sich auch die OECD mit der Bekämpfung von Computerkriminalität; vgl. beispielsweise *OECD*, Malicious Software, 2009.

[23] Hinsichtlich allgemeiner Forderungen zur Weiterentwicklung globaler Cybersicherheitsstrategien und insbesondere auch einer transnationalen und kooperativen Bekämpfung der Computerkriminalität siehe Deauville-Declaration (Renewed Commitment for Freedom and Democracy) v. 27.5.2011, Teil II (Internet); abrufbar unter: http://www.g8.utoronto.ca/summit/2011deauville/2011-declaration-en.html (Stand: 07.08.2017).

[24] Als international operierende Polizeiorganisation nimmt Interpol zwar nicht im Bereich der Rechtssetzung, aber durchaus bei der Rechtsdurchsetzung eine maßgebliche Rolle bei der Computerkriminalitätsbekämpfung wahr. Schwerpunkte bilden dabei die investigative Unterstützung der nationalen Ermittlungsbehörden, technische Analysen, Innovation und Forschung sowie die Ausbildung internationaler Teams zur Verfolgung von Cyberkriminellen.

World Trade Organisation (WTO)[25], die Weltbank[26] sowie die International Telecommunication Union (ITU)[27].

Die vorliegende Arbeit beschränkt sich allerdings aufgrund des materiellrechtlichen Ansatzes und Blickfelds auf Institutionen, die mit Normsetzungskompetenzen i. w. S. ausgestattet sind. Damit verbleiben als grundsätzlich relevante Rechtsquellen im Bereich des materiellen Computerstrafrechts völkerrechtliche Abkommen der Vereinten Nationen und des Europarates sowie das Strafrecht der Europäischen Union, da diese Institutionen – freilich mit unterschiedlicher Verbindlichkeit für die Mitgliedstaaten – gesetzgeberisch tätig werden.

B. Vereinte Nationen

Auf internationaler, transkontinentaler Ebene spielen in Bezug auf Harmonisierungsvorgänge im Bereich des materiellen Strafrechts die Vereinten Nationen allgemein, speziell der UN-Sicherheitsrat, eine maßgebliche Rolle. Daher werden die Vereinten Nationen in aller gebotenen Kürze vorgestellt. Anschließend wird auf aktuelle Entwicklungen eingegangen, die vielfach als erstmalige unmittelbare Strafrechtsetzung durch den UN-Sicherheitsrat aufgefasst wurden, bevor schließlich die Aktivitäten der Vereinten Nationen im Bereich der Computerkriminalität erläutert werden.

I. Grundstruktur der Vereinten Nationen

Die Vereinten Nationen mit Hauptsitz in New York sind die größte internationale Organisation der Welt.[28] Seit dem Beitritt des Südsudans im Jahre 2011 zählt

---

[25] Die Welthandelsorganisation befasst sich insbesondere zur Gewährleistung eines sicheren transnationalen Handels in Zeiten krimineller Aktivitäten im Cyberspace mit dem Themenfeld der Computerkriminalität; vgl. insoweit *Pontell/Geis/Brown*, International Journal of Cyber Criminology 2007, 119 (120 f).

[26] Auch die Weltbank hat ein Interesse an einer sicheren Online-Umgebung und der Entwicklung eines globalen Instruments zur Bekämpfung der Computerkriminalität; vgl. *Intven/Pfohl/Slusarchuk/Sookman*, in: The World Bank Legal Review, 2003, S. 3 (150 ff.).

[27] Zur Rolle der ITU bei der Bekämpfung der Computerkriminalität und insbesondere bei der Ausarbeitung von Modellgesetzgebung siehe *Gercke, M./Tropina*, CRi 2009, 136 ff.

[28] Unter dem Begriff der internationalen Organisationen werden aus völkerrechtlicher Perspektive zwischenstaatliche Organisationen verstanden, die unter bestimmten Voraussetzungen (auf Dauer angelegte Vereinigung von mindestens zwei selbstständigen Völkerrechtssubjekten, Tätigkeit auf dem Gebiet des Völkerrechts, selbstständige Wahrnehmung eigener Aufgaben, Ausstattung mit mindestens einem handlungsfähigen Organ) nicht nur Völkerrechtssubjekte sammeln, sondern selbst mit Rechten und Pflichten ausgestattete Völkerrechtssubjekte darstellen.

sie 193 Mitglieder. Zusätzlich gelten der Staat Palästina und der Heilige Stuhl als sog. Nichtmitglieder ohne Stimmrecht, die einen Beobachterstatus einnehmen.[29] Nach Art. 1 der Charta bezeichnen die Gewährleistung von Frieden und Sicherheit, die Entwicklung von freundschaftlichen Beziehungen zwischen den Nationen, die kooperative Bewältigung internationaler Herausforderungen und die Koordinierung von Aktionen der Völker zur Erreichung der genannten Ziele die Aufgaben und Prinzipien der Vereinten Nationen.[30]

Die Generalversammlung repräsentiert alle Mitgliedstaaten, kann jedoch lediglich völkerrechtlich nicht bindende Empfehlungen aussprechen. Die Rechtsetzungsbefugnis kommt hingegen dem Sicherheitsrat zu, der aus fünf ständigen Vetomächten und zehn weiteren, alle zwei Jahre von der Generalversammlung gewählten, mitgliedstaatlichen Vertretern zusammengesetzt ist. Als einziges UN-Organ kann der Sicherheitsrat gem. Art. 25 UN-Charta, zumindest im Bereich des Kapitels VII (Wahrung oder Wiederherstellung des Weltfriedens und der internationalen Sicherheit), die UN-Mitgliedstaaten rechtlich verpflichten.[31] Da es sich dabei regelmäßig um Einzelfälle betreffende Regelungen handelt, sind diese jedoch grundsätzlich nicht als Legislativ-, sondern als Exekutivakte einzuordnen.[32]

Neben diesen offiziellen Organen der Vereinten Nationen gibt es eine Reihe von Unterorganisationen, die sich Themen widmen, die entweder zur Gründungszeit noch nicht im Fokus der Mitgliedstaaten standen, oder die sich nicht unmittelbar aus der Charta der Vereinten Nationen ergeben.[33]

---

[29] Der sog. Beobachterstatus ist die loseste Form der Beteiligung an einer internationalen Organisation (stärkere nicht-mitgliedschaftliche Beteiligungsformen sind etwa die vertragliche bzw. mitgliedschaftliche Assoziierung, mit denen jeweils unterschiedliche Rechte und Pflichten einhergehen) und beinhaltet weder Mitsprache- noch Stimmrecht; vgl. weiterführend *Sybesma-Knol*, United Nations; *Klein/Schmahl*, in: Graf Vitzthum (Hrsg.), Völkerrecht, 4. Abschn. Rn. 89 f.

[30] Für vertiefende Hinweise vgl. *Wolfrum,* in: Simma u. a. (Hrsg.), The Charter of the United Nations, Art. 1 Rn. 1–38.

[31] Statt aller: *Epping/Menzel*, in: Ipsen (Hrsg.), Völkerrecht, 2. Kap. § 6 Rn. 150.

[32] *Klein*, in: Volger (Hrsg.), Grundlagen und Strukturen der Vereinten Nationen, S. 21 (44).

[33] Neben den zur UN-Familie zählenden Sonderorganisationen (Bsp.: UNESCO, WHO, ITU), die sämtlich durch sog. Beziehungs- und Kooperationsabkommen (Art. 57, 63 UN-Charta) mit den Vereinten Nationen verbunden und in ihrer Struktur einheitlich sind, gibt es noch sog. autonome Organisationen (Bsp.: WTO, IAEA), deren Verbindungen zu den Vereinten Nationen nicht nach dem genannten Verfahren zustande gekommen sind; vgl. eingehender zur Thematik *Epping/Menzel*, in: Ipsen (Hrsg.), Völkerrecht, 2. Kap. § 6 Rn. 180 ff.

II. Vereinte Nationen und materielles Strafrecht

Obwohl der UN-Sicherheitsrat nach klassischem Verständnis als eine Art Exekutivorgan der Vereinten Nationen ausgestaltet ist, hat er in den letzten Jahren, insbesondere nach den Terroranschlägen vom 11. September 2001, auch legislative und judikative Gewalt ausgeübt.[34] Zum einen hat er durch die Resolutionen 1373 (2001)[35] und 1540 (2004)[36] die Mitgliedstaaten der Vereinten Nationen angewiesen, konkrete strafrechtliche Verpflichtungen zur Kriminalisierung von Terrorismusfinanzierung bzw. der Herstellung von Massenvernichtungswaffen umzusetzen. Zum anderen hat er durch die Resolutionen 1267 (1999)[37], 1333 (2000)[38] und 1390 (2002)[39] Individualsanktionen verhängt.[40]

III. Vereinte Nationen und Computerkriminalität

Im Bereich der Computerkriminalität sind die Vereinten Nationen bisher nicht in gesetzgeberischer Weise tätig geworden. Das UNODC hat im Jahre 2010 die Studie „The Globalization of Crime – A Transnational Organized Crime Threat Assessment" mit einem Schwerpunkt zu Cybercrime in Kapitel 10[41] veröffentlicht. Drei Jahre später, im Februar 2013, ist die „Comprehensive Study on Cybercrime"[42] erschienen, in welcher die Herausforderungen dieses Kriminalitätsbereichs umfassend analysiert werden. Mit der Resolution 65/230 hat die Generalversammlung der Vereinten Nationen die „Commission on Crime Prevention and Criminal Justice" beauftragt, eine Expertengruppe zusammenzustellen, die

---

[34] *Macke*, UN-Sicherheitsrat und Strafrecht, S. 174.

[35] S/RES/1373(2001): Security Council Resolution 1373 (2001) on threats to international peace and security caused by terrorist acts.

[36] S/RES/1540(2004): Security Council Resolution 1540 (2004) on non-proliferation of nuclear, chemical and biological weapons.

[37] S/RES/1267(1999): Adopted by the Security Council at its 4051st meeting on 15 October 1999.

[38] S/RES/1333(2000): Security Council Resolution 1333 (2000) on measures against the Taliban.

[39] S/RES/1390(2002): Security Council Resolution 1390 (2002) on continuation of measures against the Taliban and Al-Qaida.

[40] Vgl. für einen eingehenderen Überblick *Macke*, UN-Sicherheitsrat und Strafrecht, S. 67 ff. m. w. N.

[41] *Gercke, M.*, The Globalization of Crime (UNODC), Kap. 10, 2010; abrufbar unter: http://www.unodc.org/documents/data-and-analysis/tocta/TOCTA_Report_2010_low_res.pdf (Stand: 07.08.2017).

[42] *Sieber u. a.*, Comprehensive Study on Cybercrime (UNODC), 2013; abrufbar unter: http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf (Stand: 07.08.2017).

sich mit rechtlichen und technischen Antworten auf die Computerkriminalität sowie der Rolle internationaler Institutionen befasst.

Auf dem 12. Kongress der Vereinten Nationen zur Verbrechensverhütung und Strafrechtspflege im April 2010 in Brasilien ist außerdem angedacht worden, eine weltweite UN-Konvention gegen Cyberkriminalität zu erarbeiten. Dies sahen jedoch vor allem die Unterzeichnerstaaten der Cybercrime Convention skeptisch, die eine weitere Verbreitung ihres eigenen Abkommens als Modell für nationale Regulierung vorzogen.[43] Fünf Jahre später auf dem 13. UN-Strafrechtskongress im April 2015 in Katar stellte die Bekämpfung der Cyberkriminalität abermals eines der Kernthemen dar. Der Ansatz einer globalen Anti-Cybercrime-Konvention ist jedoch mittlerweile aufgegeben und durch Plattformfunktionen[44] und sog. Capacity Building[45] auf mitgliedstaatlicher Ebene ersetzt worden.[46] Derzeitig erscheint somit eine Einflussnahme der Vereinten Nationen auf das materielle Computerstrafrecht weder durch völkerrechtlich bindende noch durch unverbindliche Modell-Abkommen in Reichweite.

C. *Europarat*

In gewisser Weise stellt der am 5. Mai 1949 gegründete Europarat mit Sitz in Straßburg ein europäisches Äquivalent zu den Vereinten Nationen dar. Mit seinen 47 Mitgliedstaaten (darunter auch alle Mitgliedstaaten der Europäischen Union) ist der Europarat die größte internationale Organisation auf dem europäischen Kontinent.

---

[43] *Hilgendorf/Valerius*, Computer- und Internetstrafrecht, § 1 Rn. 91.

[44] Das „Cybercrime Repository“ von UNODC bietet etwa eine Datenbank nationaler Rechtsakte und Urteile mit Bezug zur Cyberkriminalität und ermöglicht dadurch Mitgliedstaaten, bei der eigenen Rechtsentwicklung auf Erfahrungen anderer Staaten zurückzugreifen; abrufbar unter: https://www.unodc.org/cld/index-cybrepo.jspx (Stand: 07.08.2017).

[45] Der Begriff des *capacity building* beschreibt die Unterstützung von Entwicklungs- und Schwellenländern bei der Implementierung eines Computerstrafrechts und dessen effektiver Durchsetzung mit finanziellen Mitteln und Know-how; siehe dazu etwa die Doha-Declaration von UNODC v. 31.5.2015, A/CONF.222/L.6, S. 10 und das Discussion Paper des Europarats zu Capacity Building on Cybercrime; abrufbar unter: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802fa3e6 (Stand: 07.08.2017). Ansätze innerhalb der Vereinten Nationen gehen bereits auf das Jahr 2011 zurück; vgl. *Murray*, in: Manacorda (Hrsg.), Cibercriminality, S. 215 ff.

[46] Ein Überblick zu den aktuellen Entwicklungen auf internationaler Ebene im Rahmen des Doha-Kongresses von UNODC findet sich bei *Haase*, ZIS 2015, 422 ff.

I. Grundstruktur des Europarats und EMRK

Nach Art. 1 lit. a der Europarat-Satzung ist es dessen Aufgabe, eine engere Verbindung zwischen seinen Mitgliedstaaten zum Schutze und zur Förderung der Ideale und Grundsätze, die deren gemeinsames Erbe bilden, herzustellen und sich für deren wirtschaftlichen und sozialen Fortschritt einzusetzen. Als wesentlichste und bekannteste Errungenschaft gilt bis heute die Inkorporierung der Europäischen Konvention zum Schutz der Menschenrechte und Grundfreiheiten (EMRK) vom 4. November 1950[47] und ihrer Zusatzprotokolle. Die Sicherung des Menschenrechtsschutzes obliegt zunächst den Konventionsstaaten und ihren innerstaatlichen Rechtssystemen, da sie völkervertragsrechtlich zur Einhaltung aller in der EMRK zugesicherten Rechte verpflichtet sind.[48] In der Bundesrepublik Deutschland ist die EMRK durch Gesetz vom 7. August 1952[49] i. V. m. der Bekanntmachung vom 15. Dezember 1953 über das Inkrafttreten[50] ratifiziert worden und damit seit dem 3. September 1953 als einfaches Bundesrecht implementiert.[51] Letztlich bedeutet dies, dass sich einzelne Bürger der Mitgliedstaaten des Europarats vor ihren jeweiligen nationalen Behörden und Gerichten auf die Garantien der EMRK berufen können und die staatlichen Institutionen die Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte (EGMR) zu berücksichtigen haben.[52]

II. Europarat und materielles Strafrecht

Die EMRK bildet allerdings nur den Startpunkt für strafrechtsrelevante Initiativen des Europarats.[53] Im Jahre 1957 ist durch das Ministerkomitee der europäische Ausschuss für Strafrechtsprobleme (European Committee on Crime Pro-

---

47 Deutsche, seit 1.11.1998 geltende Fassung v. 17.5.2002, BGBl. II 2002, S. 1054 (1072).

48 Statt aller: *Hecker*, Europäisches Strafrecht, Kap. 3 Rn. 21 ff.

49 BGBl. II 1952, S. 685 (953).

50 BGBl. II 1953, S. 14.

51 Die meisten Staaten des Europarats haben die EMRK in ähnlicher Weise in ihr innerstaatliches Rechtssystem eingefügt, während etwa Österreich diese sogar mit Verfassungsrang ausgestattet hat; siehe dazu *Hecker*, Europäisches Strafrecht, Kap. 3 Rn. 21.

52 *Hecker*, Europäisches Strafrecht, Kap. 3 Rn. 21. Neben dem durch die verpflichtende Implementierung und Beachtung der EMRK durch die Konventionsstaaten bei jeglichem staatlichen Handeln bestehenden Recht eines Bürgers, sich gegenüber staatlichen Institutionen auf die Geltung der EMRK zu berufen, ist insbesondere die Möglichkeit der Individualbeschwerde durch natürliche Personen, nicht-staatliche Organisationen und Personenvereinigungen beim EGMR eine sehr weitgehende Rechtsschutzoption. Art. 34 EMRK ermöglicht den genannten Personen(-gruppen) die Rüge einer angeblichen Verletzung eines in der EMRK zugesicherten Rechts durch einen Konventionsstaat im Wege einer Individualbeschwerde; zum Verfahrensgang siehe *Hecker*, Europäisches Strafrecht, Kap. 3 Rn. 26 ff.

53 Besonders strafrechtsrelevant ist freilich Art. 6 EMRK (Recht auf ein faires Verfahren).

blems, CDCP) gegründet worden. Dessen Aufgabe besteht insbesondere darin, europäische Arbeiten zu Fragestellungen des Straf- und Strafverfahrensrechts zu koordinieren, wobei ein besonderes Augenmerk auf die internationale Zusammenarbeit in Strafsachen, in der Strafvollstreckung, im Strafvollzug, in der Kriminologie und schließlich in der Kriminalpolitik zu legen ist.[54]

Bis heute hat der Europarat mehr als 50 strafrechtsrelevante Konventionen entworfen und verabschiedet.[55] Neben der EMRK gehören zu den prominentesten vor allem das Auslieferungsübereinkommen vom 13. Dezember 1957[56], das Übereinkommen über die Rechtshilfe in Strafsachen vom 20. April 1959[57], das Übereinkommen zur Bekämpfung des Terrorismus vom 27. Januar 1977[58], das Protokoll Nr. 6 zur Konvention zum Schutze der Menschenrechte und Grundfreiheiten über die Abschaffung der Todesstrafe vom 28. April 1983[59], das Strafrechtliche Anti-Korruptionsübereinkommen vom 27. Januar 1999[60], das Übereinkommen zur Datennetzkriminalität vom 23. November 2001 (s. o. Cybercrime Convention)[61], das Übereinkommen gegen Menschenhandel vom 16. Mai 2005[62], das Übereinkommen zum Schutz von Kindern vor sexueller Ausbeutung und sexuellem Missbrauch vom 25. Oktober 2007[63] und das Übereinkommen zur Verhütung und Bekämpfung von Gewalt gegen Frauen und häuslicher Gewalt vom 11. Mai 2011[64]. Diese Konventionen unterscheiden sich einmal dadurch, dass es sich entweder um eine offene oder eine geschlossene völkerrechtliche Vereinbarung handelt. Dies bemisst sich danach, ob der Beitritt zu jener allen Völkerrechtssubjekten offensteht oder den Mitgliedern des Euro-

---

[54] *Hecker*, Europäisches Strafrecht, Kap. 3 Rn. 10.

[55] In der Originalfassung auf Englisch und Französisch können die Abkommen im Volltext unter http://www.coe.int/de/web/conventions/full-list abgerufen werden (Stand: 07.08.2017).

[56] ETS Nr. 24, BGBl. II 1964, S. 1369; II 1976, S. 1778; II 1982, S. 2071; II 1994, S. 299 mit seinen Zusatzprotokollen v. 15.10.1975 (ETS Nr. 86) und v. 17.3.1978 (ETS Nr. 98, BGBl. II 1990, S. 118; II 1991, S. 874).

[57] ETS Nr. 30, BGBl. II 1964, S. 1369 (1386); II 1976, S. 1799; II 1982, S. 2071; II 2000, S. 555 mit seinem Zusatzprotokoll v. 17.3.1978 (ETS Nr. 99, BGBl. II 1990, S. 124; II 1991, S. 909; II 2000, S. 555).

[58] ETS Nr. 90, BGBl. II 1978, S. 321 (907); II 1989, S. 857; II 1998, S. 1136 und Protokoll zur Änderung dieses Übereinkommens v. 15.5.2003 (ETS Nr. 190).

[59] ETS Nr. 114, BGBl. II 1988, S. 663; II 1989, S. 814.

[60] ETS Nr. 173 mit seinem Zusatzprotokoll v. 15.5.2003 (ETS Nr. 191).

[61] ETS Nr. 185 mit seinem Zusatzprotokoll zur Kriminalisierung von Handlungen rassistischer und fremdenfeindlicher Art begangen durch Computersysteme v. 28.1.2003 (ETS Nr. 189).

[62] ETS Nr. 197.

[63] ETS Nr. 201.

[64] ETS Nr. 210.

parats vorbehalten ist.[65] Andererseits kann im Sinne einer Zielrichtung zwischen Menschrechten garantierenden Konventionen wie der EMRK, Konventionen zur strafrechtlichen Zusammenarbeit wie dem Auslieferungsabkommen und deliktsbezogenen Konventionen wie der Cybercrime Convention abgegrenzt werden.[66]

Obwohl insbesondere die Europäische Union durch ihre Tätigkeiten im strafrechtlichen Bereich zunehmend an Bedeutung gewinnt, ist die entscheidende Rolle des Europarats weder für die Vergangenheit noch für die nähere Zukunft zu unterschätzen. Das ergibt sich vor allem aus seiner langjährigen paneuropäischen Zusammenarbeit und der damit einhergehenden Bündelung von Expertise sowie aus seinem besonders großen Adressatenkreis auf dem europäischen Kontinent und seiner Konzentration auf die Rechtsstaatlichkeit als gemeinsames Kriterium unter den Mitgliedstaaten (Art. 3 Abs. 1 Europarat-Satzung).[67] Eine besondere Leistung und Aufgabe des Europarats besteht darin, die Aufstellung und Einhaltung gesamteuropäischer Mindeststandards im Bereich des Straf- und Strafverfahrensrechts sicherzustellen.[68] Zusätzlich ist die weiter ausgreifende, aber schonendere Arbeitsweise des Europarats gegenüber der Europäischen Union hervorzuheben. Anders als die Europäische Union, die ihrer Geschichte und Zielbestimmung nach einer fortschreitenden Integration verschrieben ist und darüber hinaus mit ihren Instrumenten lediglich für die EU-Mitgliedstaaten Wirkung zeitigt, vermag es der Europarat, den gesamten europäischen Kontinent zusammenzubringen und auf niedrigschwelliger Ebene Rechtsentwicklungen anzustoßen, die in einem quasi-verfassten Staatenbund wie der Europäischen Union häufig nicht möglich sind. Die geringere Verbindlichkeit völkerrechtlicher Abkommen des Europarats gegenüber Rechtsakten der Europäischen Union stellen diesen vielfach als weniger bedrohlichen Akteur bei der Strafrechtsharmonisierung dar. Dadurch wird eine vorsichtige Angleichung des Strafrechts, auch über die Grenzen der Europäischen Union hinaus, ermöglicht.[69]

---

[65] Wenige Übereinkommen stehen ausschließlich den Mitgliedstaaten zur Unterzeichnung zur Verfügung (darunter die EMRK), wobei nicht alle der sog. offenen Übereinkommen auch nicht-europäischen Staaten gegenüber geöffnet sind; vgl. mit vertiefenden Hinweisen *Benoît-Rohmer*, Das Recht des Europarats, S. 109 ff.

[66] *Schomburg*, in: Sieber/Satzger/von Heintschel-Heinegg (Hrsg.), Europäisches Strafrecht, § 3 Rn. 1.

[67] *Hecker*, Europäisches Strafrecht, Kap. 3 Rn. 17.

[68] *Schomburg*, in: Sieber/Satzger/von Heintschel-Heinegg (Hrsg.), Europäisches Strafrecht, § 3 Rn. 23.

[69] Auch *Nuotio*, in: Dubber/Hörnle (Hrsg.), Criminal Law, S. 1115 (1130) deutet an, dass der Europarat oftmals in umfassender Weise auf Kriminalitätsfeldern aktiv werden könne, die der EU durch kompetenzrechtliche Beschränkungen verschlossen blieben.

Von der Funktionsweise her bedient sich der Europarat auf strafrechtlichem Gebiet größtenteils multilateraler Übereinkommen. Diese werden ausgearbeitet und daraufhin den Mitgliedstaaten (sog. geschlossene Konventionen) oder den Mitgliedstaaten und weiteren Völkerrechtssubjekten (sog. offene Konventionen) zum Beitritt und zur Ratifikation angeboten. Die teilnehmenden Völkerrechtssubjekte können dann, wenn zulässig, zusätzlich Vorbehalte und Erklärungen allgemeiner Art sowie auf den räumlichen Geltungsbereich bezogene Erklärungen abgeben.[70] In der Praxis besteht vielfach die Schwierigkeit, dass viele Staaten, darunter auch die Bundesrepublik Deutschland, sich zwar zunächst an der Entwicklung innovativer Modelle und Instrumente einer internationalen Strafrechtspflege im Rahmen des Europarates beteiligen und die erarbeiteten Konventionen häufig sogar unterzeichnen, jedoch letztlich die notwendige Ratifizierung auf nationalstaatlicher Ebene unterlassen, oder zumindest nicht vorantreiben.[71] Als mögliche Gründe werden in der Literatur eine fehlende parlamentarische Unterstützung, mangelnde Umsetzungskapazitäten, Nachlässigkeiten und sogar Ignoranz gegenüber praktischen Notwendigkeiten angeführt.[72] Exemplarisch hierfür steht die deutsche Unterzeichnung, aber bisher unterlassene Ratifizierung des Strafrechtlichen Anti-Korruptionsübereinkommen des Europarats vom 27. Januar 1999[73], was vor allem an einer lange Zeit fehlenden deutschen Regelung der Abgeordnetenbestechung liegt.[74] Seit der am 1. September 2014 in Kraft getretenen Änderung des § 108e StGB[75] (in der n. F. betitelt mit „Bestechung und Bestechlichkeit von Mandatsträgern“) sind die materiellen Voraussetzungen für ein Ratifikation freilich erfüllt, sodass jene in naher Zukunft zu erwarten sein dürfte.[76]

III. Europarat und Computerkriminalität

Nicht nur auf dem Gebiet der Menschen- und Verfahrensrechte hat sich der Europarat als wegweisende Organisation auf dem europäischen Kontinent, und

---

[70] *Schomburg*, in: Sieber/Satzger/von Heintschel-Heinegg (Hrsg.), Europäisches Strafrecht, § 3 Rn. 10.

[71] Vgl. *Hecker*, Europäisches Strafrecht, Kap. 3 Rn. 17.

[72] *Schomburg*, in: Sieber/Satzger/von Heintschel-Heinegg (Hrsg.), Europäisches Strafrecht, § 3 Rn. 11.

[73] ETS Nr. 173 mit seinem Zusatzprotokoll v. 15.5.2003 (ETS Nr. 191).

[74] Siehe *Wolf*, NJW 2006, 2735 (2737), mit vertiefenden Hinweisen.

[75] Änderung durch Art. 1 Nr. 4 des 48. Strafrechtsänderungsgesetzes v. 23.4.2014, BGBl. I 2014, S. 410.

[76] Bzgl. der Feinheiten des neu gefassten § 108e StGB und insbesondere dessen Umsetzung internationaler Vorgaben vgl. die umfassende Analyse bei *Heinrich*, ZIS 2016, 382 (386 ff.).

sogar zu Teilen darüber hinaus, erwiesen. Auch zu Fragen des Computerstrafrechts ist er frühzeitig tätig geworden. Schon im Rahmen der Empfehlung zu computerbezogenen Delikten vom 13. Dezember 1989[77] vertrat das Ministerkomitee die Auffassung, dass der Computerkriminalität aufgrund deren grenzüberschreitenden Dimension nur durch Harmonisierung der nationalen Strafrechtssysteme und Ausweitung der internationalen Kooperation Herr zu werden sei.[78] Als weiterer Schritt des Europarats auf dem Gebiet des Computerstrafrechts ist die Empfehlung vom 11. September 1995 zu Auswirkungen der Informationstechnologie auf das Strafverfahren[79] zu sehen, worin abermals Vorschläge an die Mitgliedstaaten zur Kooperation in Computerstrafsachen dargelegt wurden. Einen vorläufigen Höhepunkt der computerstrafrechtlichen Aktivitäten des Europarats bezeichnet die Cybercrime Convention vom 23. November 2001.[80] Diese ist am 1. Juli 2004 in Kraft getreten und wurde bis dato von 48 Staaten ratifiziert sowie von weiteren sechs Staaten unterzeichnet.[81] Die Bundesrepublik Deutschland hat die Cybercrime Convention nach Unterzeichnung am 23. November 2001 am 9. März 2009 ratifiziert.[82] Inhaltlich ist die Cybercrime Convention zweigeteilt. Auf der einen Seite beinhaltet sie das Übereinkommen über Vorgaben bezüglich strafbarer Verhaltensweisen (Art. 1 ff.) und zielt somit auf eine Harmonisierung des materiellen Strafrechts in den Unterzeichnerstaaten ab. Auf der anderen Seite enthält sie sowohl Vorgaben für das nationale Strafverfahrensrecht als auch Grundsätze internationaler Kooperation im Strafverfolgungs- und -aufklärungsbereich (Art. 14 ff.). Eine detaillierte inhaltliche Auseinandersetzung mit der Cybercrime Convention, insbesondere im Kontrast zu vergleichbaren EU-Instrumenten, folgt in Kapitel 3 § 11 E.

---

[77] Council of Europe, Recommendation No. R (89) 9 on Computer-related Crime, 1990.

[78] Vgl. *Hilgendorf/Valerius*, Computer- und Internetstrafrecht, § 1 Rn. 117.

[79] Council of Europe, Recommendation No. R (95) 13 concerning Problems of Criminal Procedure Law connected with Information Technology, 1995.

[80] Cybercrime Convention (ETS Nr. 185).

[81] Eine tagesaktuelle Liste der Ratifikations- und Unterzeichnerstaaten ist abrufbar unter: http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=Zj5AupkP (Stand: 07.08.2017).

[82] Nach Unterzeichnung wurden die Vorgaben schrittweise umgesetzt, bis die Ratifikationsurkunde Anfang 2009 beim Europarat hinterlegt werden konnte; die dazugehörige Pressemitteilung ist abrufbar unter: https://wcd.coe.int/ViewDoc.jsp?id=1416299 (Stand: 07.08.2017).

§ 2 Das materielle Strafrecht der Europäischen Union

Unter dem Terminus „Europäisches Strafrecht“ werden verschiedene Aspekte zusammengefasst,[83] zu denen auch die materiell strafrechtlichen Aktivitäten der Europäischen Union gehören. Da jedoch auch der Europarat eine herausragende Rolle bei der Schaffung von Strafrecht im europäischen Raum spielt, wird in der vorliegenden Arbeit, zur besseren Unterscheidbarkeit, für materiell strafrechtliche Aktivitäten der Europäischen Union der Begriff des „Strafrechts der Europäischen Union“ verwendet.

Die Europäische Union ist eine supranationale Institution,[84] deren Grundlage der Vertrag über die Europäische Union (EUV) und der Vertrag über die Arbeitsweise der Europäischen Union (AEUV) bilden. Beide Verträge stehen auf einer Stufe nebeneinander und werden als Europäisches Primärrecht bezeichnet.[85] Die Europäische Union steht an der Stelle der ehemaligen Europäischen Gemeinschaften, deren Rechtsnachfolgerin sie gemäß Art. 1 Abs. 3 EUV ist. Die wichtigsten Organe der Europäischen Union sind das Europäische Parlament, der Europäische Rat, der Rat, die Europäische Kommission und der Gerichtshof der Europäischen Union.

Der Vertrag von Maastricht[86] stellte durch die Einführung der Europäischen Union als „Dach“ einen wichtigen Schritt im europäischen Integrationsprozess dar, blieb aber deutlich hinter der aktuellen Konstruktion zurück. Auf dem Maastrichter Vertrag basiert auch das sog. Drei-Säulen-Modell[87], wonach die Europäische Union das Dach der drei Bereiche Europäische Gemeinschaft (EG), Gemeinsame Außen- und Sicherheitspolitik (GASP) und Polizeiliche und Justizielle Zusammenarbeit (PJZS) bildete. Die erste Säule, die EG, war bereits damals supranational ausgestaltet und explizit mit einer eigenen Rechtspersön-

---

[83] Statt vieler: *Nuotio*, in: Dubber/Hörnle (Hrsg.), Criminal Law, 2014, S. 1115 (1125).

[84] Statt aller: *Herdegen*, Europarecht, § 5 Rn. 9 f.

[85] Die Gründungsverträge (inkl. ihrer Protokolle und Anhänge) stehen gemeinsam mit ungeschriebenen Regeln (allgemeine Rechtsgrundsätze des Unionsrechts) und der Charta der Grundrechte auf primärrechtlicher Ebene des Rechts der Europäischen Union und sind im völkerrechtlichen Duktus mit Gründungsverträgen sowie im staatsanalogen Verständnis mit nationalem Verfassungsrecht vergleichbar; vgl. statt aller: *Herdegen*, Europarecht, § 8 Rn. 4 ff.

[86] Maastrichter Vertrag ist die Kurzform des am 9./10.12.1991 im niederländischen Maastricht auf dem Gipfel der Staats- und Regierungschefs vereinbarten Vertrags über die Europäische Union. Unterzeichnet wurde er am 7.2.1992 in Maastricht und trat schließlich nach seiner Ratifizierung durch alle damaligen EG-Staaten am 1.11.1993 in Kraft; siehe dazu vertiefend *Piepenschneider*, in: Bergmann (Hrsg.), Handlexikon der Europäischen Union, S. 664 ff.

[87] Statt aller: *Oppermann*, in: ders./Classen/Nettesheim (Hrsg.), Europarecht, § 3 Rn. 2; *Borchardt*, Grundlagen, § 1 Rn. 24.

lichkeit ausgestattet.[88] Im Rahmen der zweiten und dritten Säule (GASP und PJZS) hingegen wurde intergouvernemental, d. h. völkerrechtlich zusammengearbeitet, um die jeweilige einzelstaatliche Souveränität in diesen Politikbereichen möglichst wenig zu berühren.

Das sog. Lissabonner Einheitsmodell integrierte jene beiden Säulen nun in das supranationale Konstrukt. Obwohl die Rechtsfähigkeit der gesamten Europäischen Union damit nun auch im akademischen Umfeld nicht mehr streitig ist,[89] wird man sie weiterhin als Staatenverbund sui generis bezeichnen müssen, da sie zwischen einer völkerrechtlichen internationalen Organisation und einem traditionellen staatsrechtlichen Bundesstaat angesiedelt ist.[90] Für einen Bundesstaat fehlen der Europäischen Union, der Drei-Elemente-Lehre folgend, Staatsgewalt, Staatsvolk und Staatsgebiet.[91] Im Gegensatz zu anderen internationalen Organisationen kommt ihr allerdings die Fähigkeit zu, Entscheidungen auch gegen den Willen einzelner Mitgliedstaaten zu fällen.[92] Die EU-Verträge sehen Kompetenzverteilungen zwischen der Union und den Mitgliedstaaten vor, die durch das sog. Europäische Sekundärrecht auszufüllen sind.[93] Primärrechtlich sind die Handlungsformen der Europäischen Union in Art. 288 AEUV geregelt und stellen Verordnungen[94], Richtlinien[95], Beschlüsse[96] und Empfeh-

---

[88] Vgl. Art. 281 EGV a. F. und Art. 184 EAGV.

[89] Die Rechtspersönlichkeit der Europäischen Union im Völkerrecht ergibt sich aus ihrem Status als Rechtsnachfolgerin der Europäischen Gemeinschaft nach Art. 1 Abs. 3 EUV; vgl. statt vieler: *Herdegen*, Europarecht, § 5 Rn. 1 f.; *Hobe*, Europarecht, § 6 Rn. 120, während ihre Rechtsfähigkeit im innerstaatlichen (Privat-)Rechtsverkehr aus Art. 335 AEUV folgt (siehe u. a. *Herdegen*, Europarecht, § 5 Rn. 7; *Hobe*, Europarecht, § 6 Rn. 122).

[90] *Kirsch*, Demokratie und Legitimation, S. 229.

[91] Vgl. u. a. *Herdegen*, Europarecht, § 5 Rn. 15 ff.; *Oppermann*, in: ders./Classen/Nettesheim (Hrsg.), Europarecht, § 4 Rn. 18 ff., jeweils unter Bezugnahme auf *Jellinek*, Staatslehre, 1914.

[92] Vgl. *Oppermann*, in: ders./Classen/Nettesheim (Hrsg.), Europarecht, § 4 Rn. 12; *Safferling*, Internationales Strafrecht, § 9 Rn. 40.

[93] Unterhalb des Primärrechts, aber oberhalb des Sekundärrechts siedeln sich völkerrechtliche Übereinkommen der Union als Vertragspartner im System der Europäischen Unionsrechtsordnung an; vgl. *Herdegen*, Europarecht, § 8 Rn. 38.

[94] Verordnungen sind in Art. 288 Abs. 2 AEUV geregelt und von ihren rechtlichen Wirkungen her mit einem innerstaatlichen Gesetz vergleichbar, da sie unmittelbar in allen Mitgliedstaaten allgemeine Geltung und Verbindlichkeit haben und eine sog. Durchgriffswirkung auf den Einzelnen entfalten; statt aller und weiterführend: *Haag/Kotzur*, in: Bieber et al. (Hrsg.), Europäische Union, § 6 Rn. 27.

[95] Richtlinien sind in Art. 288 Abs. 3 AEUV geregelt, richten sich an die Mitgliedstaaten und verpflichten jene, den Inhalt der betreffenden Richtlinie in innerstaatliches Recht umzusetzen, wobei den Mitgliedstaaten ein gewisser inhaltlicher Gestaltungsspielraum verbleibt. Faktisch handelt es sich dabei um einen zweistufigen Prozess, da zunächst ein Regelungsprogramm durch die EU mit Verbindlichkeit für die Mitgliedstaaten erlassen wird und darauf-

lungen/Stellungnahmen[97] dar. Der für das materielle Strafrecht der Europäischen Union relevante Art. 83 AEUV sieht die Richtlinie als einschlägige Handlungsform vor. Auch das Strafrecht ist in vielfältiger Hinsicht von dessen Kompetenzzuweisungen im Mehrebenensystem betroffen,[98] was sich oftmals nicht konfliktfrei gestaltet und für den Harmonisierungsbereich der Computerkriminalität im weiteren Verlauf dieser Arbeit von zentraler Bedeutung sein wird.

A. Rechtsgrundsätze des Strafrechts der Europäischen Union

Das Verhältnis zwischen Union und Mitgliedstaaten im Sinne der Kompetenzverteilung ist maßgeblich durch geschriebene und ungeschriebene rechtliche Grundprinzipien geprägt, die auch im folgenden strafrechtlichen Kontext Bedeutung erlangen. Kodifiziert sind der Grundsatz der begrenzten Einzelermächtigung, das Subsidiaritätsprinzip und das Verhältnismäßigkeitsprinzip in Art. 5 EUV. Sie bilden die sog. europäische Schrankentrias.[99] Die Unionstreue, das Effizienzprinzip (*effet utile*) und das sog. strafrechtliche Schonungsgebot bezeichnen hingegen weitere Grundsätze, die bei der Bestimmung von Kompetenzen der Union gegenüber den Mitgliedstaaten zu beachten sind.[100] Aufgrund des strafrechtlichen Blickwinkels dieser Arbeit kann nur ein Überblick zu allgemeinen europäischen Rechtsetzungskompetenzen gegeben werden. Insbesondere auf die für strafrechtliche Harmonisierungskompetenzen relevanten Grundprinzipien des EU-Rechts wird allerdings bereits hier eingegangen, um ein Verständnis für die Funktionsweise der materiellen Strafrechtsharmonisierung zu schaffen, bevor insbesondere hinsichtlich der Auslegung des Computerkriminalitätsbegriffs in Teil 2 methodisch-argumentative Vertiefungen vorgenommen werden.

---

hin der Inhalt durch die Mitgliedstaaten in nationales Recht überführt wird (statt aller und weiterführend: *Herdegen*, Europarecht, § 8 Rn. 41 ff.; *Nettesheim*, in: Oppermann/Classen/ders. (Hrsg.), Europarecht, § 9 Rn. 82 ff.).

[96] Beschlüsse sind in Art. 288 Abs. 4 AEUV geregelt, werden grundsätzlich von der Kommission erlassen und treffen verbindliche Regelungen im Einzelfall; *Herdegen*, Europarecht, § 8 Rn. 59 f.; *Nettesheim*, in: Oppermann/Classen/ders. (Hrsg.), Europarecht, § 9 Rn. 113 ff.

[97] Empfehlungen und Stellungnahmen sind in Art. 288 Abs. 5 AEUV geregelt und entfalten zwar keine rechtliche Verbindlichkeit, sind allerdings von innerstaatlichen Gerichten insbesondere dann zu berücksichtigen, wenn sie Aufschluss über die Auslegung des Unionsrechts geben können; *Haag/Kotzur*, in: Bieber et al. (Hrsg.), Europäische Union, § 6 Rn. 38.

[98] Eine ausführliche Abhandlung zu Fragen der strafrechtlichen Kompetenzbestimmungen in Mehrebenensystemen bietet *Reinbacher*, Strafrecht im Mehrebenensystem, insb. S. 77 ff. und 365 ff.

[99] *Calliess*, in: ders./Ruffert (Hrsg.), Art. 5 EUV Rn. 5.

[100] Vgl. *Safferling*, Internationales Strafrecht, § 9 Rn. 50 ff.

I. Grundsatz der begrenzten Einzelermächtigung

In Art. 5 Abs. 1 EUV ist der Grundsatz der begrenzten Einzelermächtigung niedergelegt. Nach Art. 5 Abs. 2 EUV ist er derart ausgestaltet, dass „die Union nur innerhalb der Grenzen der Zuständigkeiten tätig [werden kann], die die Mitgliedstaaten ihr in den Verträgen zur Verwirklichung der darin niedergelegten Ziele übertragen haben. Alle der Union nicht in den Verträgen übertragenen Zuständigkeiten verbleiben bei den Mitgliedstaaten." Diese Neufassung des Art. 5 EUV durch den Vertrag von Lissabon nennt den Grundsatz der begrenzten Einzelermächtigung zum ersten Mal ausdrücklich und unterstreicht dessen Bedeutung durch die Vermutung der mitgliedstaatlichen Kompetenz in Art. 5 Abs. 2 S. 2 EUV.[101] Die explizite Festschreibung dient insbesondere auch der Abgrenzung zum begrifflichen Gegenstück der sog. Kompetenz-Kompetenz, wonach ein Normgeber seine Kompetenzen selbstständig erweitern kann.[102]

Nach der *Calliess'schen* Trias stellt der Grundsatz der begrenzten Einzelermächtigung damit die erste Schranke der Kompetenzbegründung und -ausübung durch die EU dar und legt fest, ob die Europäische Union überhaupt tätig werden darf (*Kann-Frage*).[103] Es stellt sich somit auf dieser Stufe erstens die Frage, ob der Union die Zuständigkeit zur Regelung einer bestimmten Materie zufällt, sowie zweitens, welche Handlungsformen ihr dazu zur Verfügung stehen und nach welchem Verfahren vorzugehen ist.[104]

II. Subsidiaritätsprinzip

Die zweite Stufe dieser Trias – das Subsidiaritätsprinzip – ist in Art. 5 Abs. 3 EUV geregelt. Auf dieser Stufe wird gefragt, ob die Europäische Union eine konkrete Maßnahme innerhalb einer ihr grundsätzlich zustehenden Kompetenz vornehmen darf (*Ob-Frage*).[105] Es findet eine Prüfung dahin gehend statt, ob die betreffende Maßnahme nicht auf Ebene der Mitgliedstaaten ausreichend erfolgreich durchgeführt werden kann.[106] Im Subsidiaritätsprinzip lässt sich insbesondere auch das Gebot der Achtung der nationalen Identitäten der Mitgliedstaaten aus Art. 4 Abs. 2 EUV[107] erkennen.

[101] *Hobe*, Europarecht, § 7 Rn. 183.

[102] Statt aller: *Ehlers*, in: Schulze/Zuleeg/Kadelbach (Hrsg.), Europarecht, § 11 Rn. 25.

[103] *Calliess*, in: ders./Ruffert (Hrsg.), Art. 5 EUV Rn. 5.

[104] *Nettesheim*, in: Oppermann/Classen/ders. (Hrsg.), Europarecht, § 11 Rn. 3, der auch auf die Justiziabilität der Kompetenzzuschreibung eingeht und vertiefte Hinweise zu Ausnahmen von der geschriebenen Kompetenznorm liefert („*Implied-Powers*-Lehre").

[105] *Calliess*, in: ders./Ruffert (Hrsg.), Art. 5 EUV Rn. 5.

[106] *Hobe*, Europarecht, § 7 Rn. 189; *Nettesheim*, in: Oppermann/Classen/ders. (Hrsg.), Europarecht, § 11 Rn. 23 ff.

[107] Zur Identitätsklausel ausführlich *von Bogdandy/Schill*, ZaöRV 2010, 701 ff.

Das Subsidiaritätsprinzip trägt daher den Aspekten einer vorsichtigen Übertragung von Hoheitsrechten durch die Mitgliedstaaten auf die Europäische Union Rechnung. Für das Strafrecht der Europäischen Union bedeutet dies, dass eine Harmonisierung nur dann in Betracht kommen kann, wenn sie im Vergleich zu einem mitgliedstaatlichen Tätigwerden „unerlässlich" ist, weshalb auch von einer „Kompetenzausübungsmaxime" gesprochen wird.[108] Umgesetzt wird das Subsidiaritätsprinzip mithilfe des sog. Erforderlichkeits- und Effizienztests, bei dem erstens zu prüfen ist, ob ein Unionsziel nur durch ein Tätigkeitwerden der EU zu erfüllen ist (sog. Negativkriterium), und zweitens, ob dadurch ein Mehrwert für die Zielerreichung erlangt wird (sog. Positivkriterium).[109]

Ein grundsätzliches Konstruktionsproblem des Subsidiaritätsprinzips und der dazugehörigen Tests besteht darin, dass diese auf den Zielen der betreffenden Maßnahme aufbauen. Das heißt, dass die Europäische Union lediglich einen einheitlichen europäischen Rechtszustand als Ziel ausgeben muss, um den begrenzenden Charakter der Subsidiaritätstests zu unterlaufen.[110] Denn dieses Ziel kann auf mitgliedstaatlicher Ebene denklogisch nie erreicht werden.[111]

III. Verhältnismäßigkeitsprinzip

Auf dritter Stufe der europäischen Schrankentrias zur Kompetenzbegründung und -ausübung steht das Verhältnismäßigkeitsprinzip des Art. 5 Abs. 4 EUV. Danach dürfen die jeweiligen Organe der Europäischen Union nicht über das zur Erreichung der Ziele der Verträge erforderliche Maß hinausgehen (*Wie-Frage*).[112] Das Prinzip eines verhältnismäßigen Handelns der Europäischen Union war vom EuGH schon vor seiner Kodifizierung im EG-Vertrag als allgemeiner Grundsatz des europäischen Rechts anerkannt worden.[113] Im Gegensatz zum Subsidiaritätsprinzip ist das Verhältnismäßigkeitsprinzip eine „Kompetenzausübungsregelung", sodass bei Vorliegen mehrerer Handlungsalternativen die mildeste Möglichkeit zu wählen ist.[114]

---

[108] *Haratsch/Pechstein/Koenig*, Europarecht, 2. Kap. Rn. 166.

[109] *Calliess*, in: ders./Ruffert (Hrsg.), Art. 5 EUV Rn. 5; *Hecker*, Europäisches Strafrecht, Kap. 8 Rn. 50; *Hobe*, Europarecht, § 7 Rn. 191 f.

[110] *Nettesheim*, in: Oppermann/Classen/ders. (Hrsg.), Europarecht, § 11 Rn. 31.

[111] Stattdessen wird etwa von *Deakin*, ELJ 12 (2006), 440 ff., die Idee des Wettbewerbs der Rechtssysteme und der Heterogenität vorgeschlagen, um dem Subsidiaritätsprinzip besser gerecht zu werden.

[112] Vgl. *Calliess*, in: ders./Ruffert (Hrsg.), Art. 5 EUV Rn. 5.

[113] EuGH, Rs. C-359/92, Slg. 1994, I-3683 – *Deutschland/Rat*.

[114] *Geiger*, Strafrechtsharmonisierung, S. 52 m. w. N.

Der europäische Verhältnismäßigkeitsgrundsatz stimmt nicht mit demjenigen des deutschen Rechts überein, da der EuGH die Zweck-Mittel-Relation (Angemessenheit) zwar nicht als Prüfungskriterium ausschließt, sie jedoch bislang lediglich zurückhaltend anwendet.[115] Im deutschen Rechtsverständnis stellt die Angemessenheitsprüfung hingegen regelmäßig die entscheidende Rechtmäßigkeitshürde dar.

IV. Effizienzprinzip (effet utile)

Der primärrechtlich in Art. 4 Abs. 3 EUV zum Ausdruck kommende Grundsatz des *effet utile* geht auf einen Rechtsgedanken des Wiener Übereinkommens vom 23. Mai 1969 über das Recht der Verträge (WÜV) zurück.[116] Im EU-Recht findet er regelmäßig als eine Art teleologische Auslegungsregel[117] Anwendung, wonach die größtmögliche „praktische Wirksamkeit"[118] oder „nützliche Wirkung"[119] des Unionsrechts erreicht werden soll. In der EU-rechtlichen Praxis haben sich aus dem *effet-utile*-Grundsatz Leitmotive entwickelt, die sich vor allem in der Gewährleistung von Gleichheit, Freiheit, Solidarität und Einheit ausdrücken lassen.[120] Im Verhältnis zwischen nationalem Recht und EU-Recht bedeutet eine konsequente Anwendung des Effizienzprinzips freilich eine „größtmögliche Ausschöpfung"[121] der EU-Kompetenzen.[122] Dieser Blickwinkel auf den *effet-utile*-Grundsatz macht zweierlei deutlich. Erstens haben nationalstaatliche Rechtsordnungen im Konfliktfall hinter dem EU-Recht zurückzustehen, da nur dann dessen volle Wirksamkeit gewährleistet wird, und zweitens verschafft sich das EU-Recht durch das Gebot einer *effet-utile*-Interpretation den Freiraum für weitere dynamische Rechtsentwicklungen.[123]

---

[115] *Nettesheim*, in: Oppermann/Classen/ders. (Hrsg.), Europarecht, § 11 Rn. 33.

[116] *Safferling*, Internationales Strafrecht, § 9 Rn. 70.

[117] *Calliess*, ZEuS 2008, 3 (7); *Ritzer*, Europäische Kompetenzordnung, S. 64.

[118] Vgl. etwa EuGH, Rs. C-48/75, Slg. 1976, 497 (517) – *Noël Royer*; Rs. C-792/79, Slg. 1980, 119 (131) – *Camera Care*; Rs. C-246/80, Slg. 1981, 2311 (2328) – *Broekmeulen*.

[119] Vgl. etwa EuGH, Rs. 9/70, Slg. 1970, 825 (838) – *Leberpfennig*; Rs. 187/87, Slg. 1988, 5013 ff. – *Saarland u. a./Minister für Industrie, Post- und Fernmeldewesen und Fremdenverkehr u. a.*; Rs. C-434/97, Slg. 2000, I-1129 – *Kommission/Frankreich*; siehe auch BVerfGE 6, 55 (72).

[120] *Borchardt*, in: Schulze/Zuleeg/Kadelbach (Hrsg.), Europarecht, § 15 Rn. 47.

[121] BVerfGE 89, 155 (210).

[122] *Reinbacher*, Strafrecht im Mehrebenensystem, S. 424.

[123] *Reinbacher*, Strafrecht im Mehrebenensystem, S. 425.

V. Unionstreue

Ein weiteres, sich aus Art. 4 EUV ergebendes Strukturprinzip stellt die Unionstreue dar, die sich gewissermaßen als Gegenstück zur Achtung der nationalen Identitäten der Mitgliedstaaten verstehen lässt.[124] Aufgrund der weitgehenden Unbestimmtheit und des hohen Abstraktionsgrads des Begriffs der Unionstreue sind gewisse Unterkategorien gebildet worden, denen sich dann bestenfalls Handlungsempfehlungen und -anweisungen für die beteiligten Akteure im Mehrebenensystem der Europäischen Union entnehmen lassen.[125] Aus diesem abstrakten Begriff ableitbare und anerkannte Subprinzipien[126] sind beispielsweise das Kooperationsprinzip,[127] das den Mitgliedstaaten gewisse Handlungspflichten auferlegt, und das Rücksichtnahmegebot,[128] das Unterlassungspflichten für die mitgliedstaatliche Ebene statuiert. Als Konkretisierungen dieser Subprinzipien – und damit letztlich des Gebots der Unionstreue – lassen sich insbesondere die Pflicht zur unionsrechtskonformen Auslegung des nationalen Rechts[129] und der Grundsatz des Vorrangs des Unionsrechts[130] ausmachen.

VI. Strafrechtliches Schonungsgebot

Einen Unterfall der Achtung der nationalen Identitäten der Mitgliedstaaten und des Subsidiaritätsprinzips stellt der sog. strafrechtliche Schonungsgrundsatz[131] dar. Dieser von *Satzger* geprägte Begriff ist seither in der deutschen europastrafrechtlichen Literatur mehrfach aufgegriffen worden.[132] Auch das Bundesverfassungsgericht hat sich das strafrechtliche Schonungsgebot mittlerweile zu eigen gemacht.[133] Es verlangt der Europäischen Union insbesondere bei strafrechtlichen Maßnahmen eine besondere Rücksicht auf nationale Besonderheiten ab. Dabei bleibt jedoch unklar, inwieweit sich eine besondere Berücksichtigung der

---

[124] *Safferling*, Internationales Strafrecht, § 9 Rn. 74 ff., auch mit vertiefenden Hinweisen.

[125] *Marauhn*, in: Schulze/Zuleeg/Kadelbach (Hrsg.), Europarecht, § 7 Rn. 13.

[126] Die Terminologie geht zurück auf *Kahl*, in: Calliess/Ruffert (Hrsg.), Art. 4 EUV Rn. 39.

[127] *Kahl*, in: Calliess/Ruffert (Hrsg.), Art. 4 EUV Rn. 39; *Marauhn*, in: Schulze/Zuleeg/Kadelbach (Hrsg.), Europarecht, § 7 Rn. 13; *Streinz*, in: ders. (Hrsg.), Art. 4 EUV Rn. 1.

[128] *Kahl*, in: Calliess/Ruffert (Hrsg.), Art. 4 EUV Rn. 40; *Marauhn*, in: Schulze/Zuleeg/Kadelbach (Hrsg.), Europarecht, § 7 Rn. 13; *Streinz*, in: ders. (Hrsg.), Art. 4 EUV Rn. 1.

[129] Siehe unten, Kap. 2 § 7 C. I. 2.

[130] Siehe unten, Kap. 2 § 7 C. I. 1.

[131] Erstmals grundlegend dazu *Satzger*, Europäisierung des Strafrechts, S. 166 ff.

[132] *Ambos*, Internationales Strafrecht, § 11 Rn. 35; *Böse*, ZIS 2010, 76 (85); *Esser*, Europäisches und Internationales Strafrecht, § 2 Rn. 157; *Hecker*, in: Sieber/Satzger/von Heintschel-Heinegg (Hrsg.), Europäisches Strafrecht, § 10 Rn. 44; *ders.*, Europäisches Strafrecht, Kap. 8 Rn. 55; *Zimmermann*, JURA 2009, 844 (849).

[133] Vgl. BVerfGE 123, 267 (360).

sozio-kulturellen Wertvorstellungen, die sich im jeweiligen mitgliedstaatlichen Strafrecht niedergeschlagen haben, von der allgemeinen Achtung der nationalen Identitäten unterscheidet, sodass es sich bei der Forderung nach Beachtung eines strafrechtlichen Schonungsgebots grundsätzlich um einen kriminalpolitischen Appell handelt, der die Grundsätze des Art. 4 EUV aufgreift.[134] Regelmäßig wird dabei vorgetragen, dass das nationale Strafrecht infolge seiner Grundrechtsrelevanz eine derart sensible Rechtsmaterie darstellt, dass eine Sonderbehandlung im Integrationsprozess gerechtfertigt sei,[135] um gesellschaftspolitischen und kulturellen Eigenheiten der Mitgliedstaaten gerecht zu werden.[136]

Ob der sog. Notbremsemechanismus des Art. 83 Abs. 3 AEUV möglicherweise eine prozessuale Ausgestaltung des strafrechtlichen Schonungsgrundsatzes ist,[137] und wie sich dieses Instrument allgemein in den Auslegungsvorgang im Mehrebenensystem der Europäischen Union einordnen lässt, wird wesentlicher Bestandteil des dritten Teils dieser Arbeit sein.[138]

Obgleich der strafrechtliche Schonungsgrundsatz durch die deutsche Strafrechtswissenschaft entwickelt wurde, ist davon auszugehen, dass auch die EU-Institutionen grundsätzlich anerkennen, dass die Strafrechtssysteme der Mitgliedstaaten einem besonderen Souveränitätsschutz zu unterliegen haben.[139] Bereits das Grünbuch der EU stellt fest, dass Dissonanzen entstünden, wenn einzelne nationale Bestandteile ohne Rücksicht auf die Gesamtstruktur eines Mitgliedstaats verändert würden, da das Strafrecht „historisch, kulturell und rechtlich […] fest mit dem jeweiligen Rechtssystem verbunden [ist]".[140]

B. *Europäische Union und materielles Strafrecht*

Die Europäische Union ist aufgrund des o. g. Subsidiaritätsgrundsatzes nur in sehr engen Grenzen dazu berufen und kompetent, selbstständig Kriminalstrafrecht zu schaffen.[141] Die Mitgliedstaaten als „Herren der Verträge" haben der Europäischen Union lediglich in Art. 325 Abs. 4 AEUV die Kompetenz übertragen, „die erforderlichen Maßnahmen zur Verhütung und Bekämpfung von Be-

---

[134] Vgl. *Satzger*, Internationales und Europäisches Strafrecht, § 9 Rn. 9.
[135] Vgl. *Zimmermann*, JURA 2009, 844 (849) m.w.N.
[136] *Satzger*, Europäisierung des Strafrechts, S. 169.
[137] So *Kotzur*, in: Geiger/Khan/ders. (Hrsg.), Art. 83 AEUV, Rn. 12.
[138] Siehe unten, Kap. 3 § 12 D. II. 2.
[139] Vgl. *Schaut*, Europäische Strafrechtsprinzipien, S. 99.
[140] KOM (2004) 334 endg., S. 8.
[141] Statt vieler: *Heinrich*, Strafrecht AT, Rn. 80a.

trügereien, die sich gegen die finanziellen Interessen der Union richten“, zu ergreifen – auch durch Setzung kriminalstrafrechtlicher Normen.[142]

Daneben ist dem Strafrecht der Europäischen Union im engeren Sinne allerdings auch das sog. Strafanweisungsrecht zuzurechnen.[143] Dies sind Rahmenbeschlüsse[144] und Richtlinien der Europäischen Union, welche die nationalen Gesetzgeber verpflichten, Strafnormen zu schaffen, die dann wiederrum unmittelbare Wirkung gegenüber den Rechtsunterworfenen entfalten.[145]

Schließlich wird der Begriff des Strafrechts der Europäischen Union im weiteren Sinne für einzelstaatliche Normen verwendet, die durch Umsetzung früherer Richtlinien oder Rahmenbeschlüsse „europäisiert“ worden sind.[146]

Beispielhaft stehen für diesen Bereich des Strafrechts der Europäischen Union die §§ 202a, 202b, 202c und 303b StGB. Diese Straftatbestände sind durch das 41. StrÄndG[147] *in das StGB aufgenommen worden und setzen dabei den Rahmenbeschluss 2005/222/JI über Angriffe auf Informationssysteme*[148] *um. Insbesondere das Hacking wurde in § 202a StGB als Ausspähung von Daten durch das Strafrecht der Europäischen Union in Deutschland kriminalisiert.*

Das Strafrecht der Europäischen Union i. w. S. umfasst mithin sowohl das Strafanweisungsrecht selbst als auch diejenigen nationalstaatlichen Normen, die aufgrund des Unionsrechts implementiert bzw. verändert worden sind.

Im Folgenden wird jedoch allein das Strafrecht der Europäischen Union i. e. S. (insbesondere das sog. Strafanweisungsrecht) behandelt.

I. Materielles Strafrecht der EU „Prä-Lissabon“

Lange Zeit führte das materielle Strafrecht auf Ebene der Europäischen Union ein Schattendasein. Während andere Politikbereiche schon zuvor vielfältigen Europäisierungs- und Integrationsbemühungen ausgesetzt waren, rückte das Straf-

---

[142] *Hecker*, Europäisches Strafrecht, Kap. 1 Rn. 34; vor Inkrafttreten des Vertrags von Lissabon fand sich lediglich in Art. 280 EGV a. F. die Verpflichtung der Mitgliedstaaten, die finanziellen Interessen der Europäischen Gemeinschaft gleich ihren eigenen zu schützen; siehe etwa *Heger*, ZIS 2007, 547 (550) m. w. N.

[143] *Safferling*, Internationales Strafrecht, § 9 Rn. 6; *Sieber*, in: ders./Satzger/von Heintschel-Heinegg (Hrsg.), Europäisches Strafrecht, Einf. Rn. 4.

[144] Das EU-Instrument des Rahmenbeschlusses ist durch den Vertrag von Lissabon durch die Richtlinie ersetzt worden.

[145] *Sieber*, in: ders./Satzger/von Heintschel-Heinegg (Hrsg.), Europäisches Strafrecht, Einf. Rn. 4.

[146] *Ambos*, Internationales Strafrecht, § 9 Rn. 4; *Hecker*, Europäisches Strafrecht, Kap. 1 Rn. 5.

[147] 41. StrÄndG v. 7.8.2007, BGBl. I 2007, S. 1786 f.

[148] ABl. L 69 v. 16.3.2005, S. 67 ff.

recht erst mit Inkrafttreten des Vertrags von Amsterdam am 1. Mai 1999[149] in den Fokus der Europäisierung.[150] Durch die Schaffung des Unionsziels, einen „Raum der Freiheit, der Sicherheit und des Rechts" zu bilden, sind das Strafrecht und dessen Harmonisierung Teil der europäischen Agenda geworden.[151]

Bis zum Inkrafttreten des Vertrags von Lissabon war das Strafrecht der EU in der sog. dritten Säule (Art. 29–53 EUV a.F.) geregelt, wobei sich gewisse strafrechtliche Kompetenzen auch aus der ersten Säule ergaben. So hätte in Bezug auf die Regelungsmaterie der ersten Säule – anders als bei der PJZS – mit der Verordnung auch ein Mittel zur Schaffung unmittelbar wirkender Strafrechtsnormen bestanden, jedoch gingen sowohl die herrschende Lehre als auch die Praxis damals davon aus, dass eine zur Schaffung unmittelbar wirkender Strafrechtsnormen nötige Kompetenz weder im Rahmen der ersten noch im Rahmen der dritten Säule bestand.[152]

Eine Anweisungskompetenz, also die Möglichkeit durch europäische Regelungsvorgaben auf die nationalstaatlichen Strafrechtssysteme Einfluss zu nehmen, sahen dagegen sowohl die erste als auch die dritte Säule der EU seit dem Inkrafttreten des Vertrags von Maastricht vor. In der dritten Säule standen dazu zwei Handlungsformen zur Verfügung: Rahmenbeschlüsse nach Art. 34 Abs. 2 lit. b EUV a.F. sowie Übereinkommen nach Art. 34 Abs. 2 lit. d EUV a.F.[153] Weniger direkt ersichtlich, aber doch durch den EuGH ausdrücklich positiv entschieden,[154] standen auch im Rahmen der ersten Säule mit Richtlinien, Verordnungen und Entscheidungen nicht nur geeignete Handlungsformen bereit, sondern die EU hatte auch die nötige Anweisungskompetenz, um nationalstaatliches Strafrecht zu beeinflussen.[155]

Derartige Rechtsakte der Europäischen Union im Bereich des materiellen Strafrechts sind vor Inkrafttreten des Vertrags von Lissabon vor allem durch zahlreiche Rahmenbeschlüsse ergangen, z.B. zur Bekämpfung der Geldwä-

---

[149] ABl. C 340 v. 10.11.1997, S. 1.

[150] In der Früh- und Mittelzeit der europäischen Einigung zwischen Schuman-Plan, Montanunion und den Römischen Verträgen fanden sich lediglich implizite Hinweise auf Europäisierungstendenzen im Strafrecht; siehe weiterführend *Heger*, in: Giegerich (Hrsg.), Herausforderungen und Perspektiven der EU, S. 157.

[151] *Kaiafa-Gbandi*, ZIS 2006, 521.

[152] *Calliess*, ZEuS 2008, 3 (16); *Dorra*, Legislativkompetenzen, S. 40 und 147; *Zöller*, ZIS 2009, 340 (343).

[153] *Calliess*, ZEuS 2008, 3 (13); *Dannecker*, JURA 2006, 95 (99); *Muñoz*, eucrim 2008, 73 (75).

[154] EuGH, Rs. C-176/03, Slg. 2005, I-07879 – *Umweltstrafrecht*, Rs. C-308/06, Slg. 2008, I-04057 – *Meeresverschmutzung*.

[155] *Dorra*, Legislativkompetenzen, S. 148 m.w.N. zu den einzelnen Rechtsinstrumenten und ihrer Nutzbarmachung im Rahmen strafrechtlicher Anweisungen.

sche[156], der Geldfälschung[157], des Terrorismus[158], des Menschenhandels[159], des Drogenhandels[160], der Computerkriminalität[161], der organisierten Kriminalität[162] und des Rassismus[163].

II. Materielles Strafrecht der EU „Post-Lissabon“

Der am 1. Dezember 2009 in Kraft getretene Vertrag von Lissabon hat der Europäischen Union nicht nur eine eigenständige Rechtspersönlichkeit verliehen, sondern darüber hinaus das oben beschriebene Säulen- oder Tempelmodell abgeschafft und durch eine einheitliche Europäische Union ersetzt. Sämtliche Kompetenzen der Europäischen Union sind nun in den zwei grundlegenden EU-Verträgen, einerseits im Vertrag über die Europäische Union (EUV) und andererseits im Vertrag über die Arbeitsweise der Europäischen Union (AEUV), geregelt.

Die justizielle Zusammenarbeit in Strafsachen, die vormals in der dritten Säule eingegliedert war, findet sich nun in den Art. 82–86 AEUV, wobei aus materiell-strafrechtlicher Perspektive vornehmlich Art. 83 AEUV relevant ist. Durch die Neuordnung im Rahmen des Vertrags von Lissabon hat das Strafrecht der EU tief greifende Änderungen erfahren. Die Wechsel des Harmonisierungsmittels vom Rahmenbeschluss zur Richtlinie stärkt die demokratische Legitimation und schwächt gleichzeitig die Position der Mitgliedstaaten. Für Richtlinien ist nämlich das ordnungsgemäße Gesetzgebungsverfahren einschlägig, sodass nach den Art. 289 Abs. 1, 294 AEUV der Rat und das Europäische Parlament gemeinsam zuständig sind, während im Rahmen der dritten Säule das Parlament lediglich anzuhören war (Art. 39 Abs. 1 S. 1 EUV a.F.).[164] Darüber hinaus genügt bei einer Abstimmung über eine solche Richtlinie im Rat nach Art. 16 Abs. 3 EUV nun eine einfache Mehrheit, wohingegen Rahmenbeschlüsse nach Art. 34 Abs. 2 S. 2 EUV a.F. nur einstimmig ergehen konnten. Dagegen steht das Initiativrecht zu einer strafrechtlichen Richtlinie neben der Kommission nach Art. 76 AEUV jetzt nur einer Gruppe von einem Viertel aller

---

[156] Rahmenbeschluss 2001/500/JI v. 26.6.2001, ABl. L 182 v. 5.7.2001, S. 1.

[157] Rahmenbeschluss 2001/888/JI v. 6.12.2001, ABl. L 329 v. 14.12.2001, S. 3 und Rahmenbeschluss 2001/413/JI v. 28.5.2001, ABl. L 149 v. 2.6.2001, S. 1.

[158] Rahmenbeschluss 2002/475/JI v. 13.6.2002, ABl. L 164 v. 22.6.2002, S. 3 und Rahmenbeschluss 2008/919/JI v. 28.11.2008, ABl. L 330 v. 9.12.2008, S. 21.

[159] Rahmenbeschluss 2002/629/JI v. 19.7.2002, ABl. L 203 v. 1.8.2002, S. 1.

[160] Rahmenbeschluss 2004/757/JI v. 25.10.2004, ABl. L 335 v. 11.11.2004, S. 8.

[161] Rahmenbeschluss 2005/222/JI v. 24.2.2005, ABl. L 69 v. 16.3.2005, S. 67.

[162] Rahmenbeschluss 2008/841/JI v. 24.10.2008, ABl. L 300 v. 11.11.2008, S. 42.

[163] Rahmenbeschluss 2008/913/JI v. 28.11.2008, ABl. L 1328 v. 6.12.2008, S. 55.

[164] *Sieber*, ZStW 121 (2009), 1 (60).

Mitgliedstaaten zu, während nach Art. 34 Abs. 2 S. 2 EUV a. F. bereits ein einzelner Mitgliedstaat aktiv werden konnte. Dadurch ist die Macht eines einzelnen Mitgliedstaats begrenzt worden. Schließlich ist nach dem Vertrag von Lissabon nun bezüglich der Umsetzung strafrechtlicher EU-Richtlinien gem. Art. 258 ff. AEUV die Anstrengung eines Vertragsverletzungsverfahrens gegen die Mitgliedstaaten statthaft, was bei Rahmenbeschlüssen nicht der Fall war.[165]

Nicht nur im bislang sehr eng begrenzten Bereich der Strafrechtsetzungskompetenz nimmt die Regelungsweite des Strafrechts der Europäischen Union fortwährend zu.[166] Anlässlich dieser Gleichstellung der strafrechtlichen Kompetenzen mit anderen Politikbereichen der EU ist, der dynamischen Entwicklung des EU-Rechts folgend, eine weitere Zunahme harmonisierender Rechtsakte auch im Sicherheitsbereich überwiegend wahrscheinlich.[167] Darauf deuten auch die politischen Absichten der EU-Institutionen hin.[168] Insbesondere der Bereich der Computerkriminalität als modernes Kriminalitätsfeld mit vielen transnationalen Elementen wird auch in den kommenden Jahren und Jahrzehnten Harmonisierungsbestrebungen ausgesetzt sein. Um einerseits Art und Umfang zukünftiger Harmonisierungsakte abschätzen zu können und andererseits das Zusammenwirken unionsrechtlicher und verfassungsrechtlicher Prinzipien zu verdeutlichen, ist eine Auseinandersetzung mit den Prinzipien der Strafrechtsharmonisierung im EU-Recht angezeigt.

1. Prinzipien europäischer Strafrechtsharmonisierung

Als Grundbedingung für strafrechtliche Harmonisierungen sind sowohl verfassungsrechtliche Aspekte auf mitgliedstaatlicher Seite als auch europarechtliche Vorgaben relevant.[169]

Verfassungsrechtlich betrachtet ist in der Kompetenz zur Harmonisierung von Strafrecht eine Übertragung von Hoheitsrechten der Mitgliedstaaten auf die Europäische Union zu sehen. Diese muss aus deutscher Sicht den Voraussetzun-

---

[165] *Zimmermann*, JURA 2009, 844 (844).

[166] So schon damals *Velten*, in: Jayme/Mansel/Pfeiffer (Hrsg.), Jahrbuch für Italienisches Recht Bd. 20, 2007, S. 173 (183); *Vervaele*, in: Demaret u. a. (Hrsg.), European Legal Dynamics, 2007, S. 279 (298).

[167] Vgl. bereits *Harms*, in: Juristische Studiengesellschaft Karlsruhe (Hrsg.), Jahresband 2007, S. 173 (189) und aktuell *Hecker*, in: Sieber/Satzger/von Heintschel-Heinegg (Hrsg.), Europäisches Strafrecht, § 10 Rn. 3.

[168] Die EU-Kommission etwa möchte die „ungeahnten Möglichkeiten" des Rechtsrahmens post-Lissabon zur Bekämpfung „sämtliche[r] Sicherheitsbedrohungen […] so weit irgend möglich" nutzen; Mitteilung der Kommission zum Raum der Freiheit, der Sicherheit und des Rechts v. 20.4.2010, KOM (2010) 171, S. 6.

[169] Vgl. dazu *Asp u. a.*, (Manifest Kriminalpolitik), ZIS 2009, 697 ff.

gen des Art. 23 Abs. 1 GG Rechnung tragen, also erstens den Integrationsauftrag des Grundgesetzes, zweitens die Sicherung der Struktur des Grundgesetzes und drittens die Bewahrung dessen unveräußerlichen Verfassungskerns beachten.[170]

Exkurs: Nach einem aktuellen Beschluss des Bundesverfassungsgerichts zum Europäischen Haftbefehl[171] gehört zum unveräußerlichen Verfassungskern – durch seine Verwurzelung in der Menschenwürdegarantie des Art. 1 Abs. 1 GG – namentlich auch der Schuldgrundsatz. Welche Auswirkungen dieser Beschluss auf zukünftige strafrechtliche Harmonisierungen, den europäischen Verfassungsgerichtsdialog,[172] *Ultra-vires-Verfahren*[173] und gegebenenfalls auch für die Zuordnung der Interpretationshoheit bezüglich des Unionsrechts[174] haben wird, ist freilich noch nicht abzusehen. Allerdings deutet das Vorgehen des Bundesverfassungsgerichts bereits jetzt darauf hin, dass trotz weitreichender Souveränitätspreisgaben durch strafrechtliche Kompetenznormen im EU-Primärrecht zumindest im Einzelfall grundrechtliche Anforderungen zu beachten bleiben. Möglicherweise könnte durch die Zuordnung des Schuldprinzips zur Menschenwürdegarantie des Art. 1 Abs. 1 GG[175] und die damit verbundene verfassungsrechtliche Unveräußerlichkeit ein Konflikt mit dem höherrangigen Unionsrecht vermieden worden sein. Dadurch hätte das Bundesverfassungsgericht nämlich nicht entschieden, dass ein *Ultra-vires*-Handeln der Europäischen Union vorliegt, sondern stattdessen erkannt, dass diese Ausnahme im EU-Auslieferungsrecht schon ursprünglich vorgesehen war, da ansonsten schließlich die Identitätsklausel verletzt wäre. Der Argumentation des Bundesverfassungsgerichts folgend ist in dieser Konstruktion auch keine versteckte Kompetenzüberschreitung des Bundesverfassungsgerichts durch die faktische Auslegung von Unionsrechts zu erkennen.[176] Zumindest bezüglich des Europäischen Haftbefehls hat sich der EuGH der Herausforderung des Bundesverfassungsgerichts unmittelbar gestellt und

[170] Diese Grundkonzeption zur Einbindung der Bundesrepublik Deutschland innerhalb der Europäischen Union zieht sich durch die gesamte Argumentation des Lissabon-Urteils. Einerseits wird dadurch die Verfassungsmäßigkeit der partiellen Souveränitätspreisgabe Deutschlands begründet und andererseits werden die verfassungsimmanenten Grenzen für zukünftige Integrationsschritte festgelegt; vgl. insoweit insb. BVerfGE 123, 267 (350 ff.).

[171] BVerfG NJW 2016, 1149–1162; dabei stellte sich die Frage, ob ein in Deutschland aufgegriffener und zuvor von einem italienischen Gericht in Abwesenheit Verurteilter ausgeliefert werden kann, obwohl nicht sichergestellt ist, dass bei einem etwaigen Berufungsprozess auch die Argumente des Beschuldigten zur Sache aufgenommen würden.

[172] Vgl. zum Europäischen Verfassungsgerichtsdialog unten, Kap. 2 § 7 C. I. 2. b. cc.

[173] Siehe zum *Ultra-vires*-Verfahren unten, Kap. 2 § 7 C. I. 1. b.

[174] Siehe insoweit unten, Kap. 1 § 7 C. I 1.

[175] BVerfG NJW 2016, 1149 (1150, 1152 f.).

[176] Durch die Zuordnung des Schuldprinzips zur Menschenwürdegarantie entzieht sich das BVerfG der Vorrangwirkung des EU-Rechts, indem es das Prinzip dem unveräußerlichen Verfassungskern zuschreibt und dadurch der Interpretationskompetenz des EuGH entzieht. Auf diese Weise macht das BVerfG aus der EU-rechtlich geregelten Fragestellung, ob eine Person nach einem Abwesenheitsprozess in Italien und einer fehlenden zweiten Tatsacheninstanz ausgeliefert werden darf, eine verfassungsrechtliche. Das BVerfG argumentiert (vereinfacht dargestellt), dass das Unionsrecht schließlich die nationalen Identitäten achte und somit eine Missachtung des Schuldprinzips/der Menschenwürde schlicht undenkbar sei. Somit sei an dieser Stelle die Auslegung des EU-Rechts so eindeutig, dass auch das eigentlich

in einem Vorabentscheidungsverfahren auf Vorlage des OLG Bremen[177] die grund- und menschenrechtlichen Argumente des Bundesverfassungsgerichts aufgenommen.[178] Gleichwohl argumentiert der EuGH strikt unionsrechtlich, leitet die vom Bundesverfassungsgericht geforderten Schutzstandards aus den europäischen Grundrechten her und nimmt der Identitätskontroll-Drohung des Bundesverfassungsgerichts damit den Wind aus den Segeln.[179]

Aus europarechtlicher Perspektive spielen die oben bereits genannten Prinzipien der begrenzten Einzelermächtigung, der Subsidiarität und der Verhältnismäßigkeit sowie die Pflicht zur Achtung der nationalen Identitäten jeweils eine beschränkende Rolle, während die Unionstreue und das Effizienzprinzip tendenziell integrationsfördernd wirken. Über diese allgemeinen unionsrechtlichen und zur Kompetenzabgrenzung notwendigen Grundsätze hinaus hat die Europäische Union jedoch keine, den mitgliedstaatlichen Rechtsordnungen vergleichbare oder gar gleichwertige, strafrechtsspezifische Prinzipienstruktur zur Entwicklung eines Strafrechts der Europäischen Union herausgebildet.[180] Welche Auswirkungen diese Tatsache für die Interpretationskompetenzen im Mehrebenensystem zwischen den nationalen und europäischen Gerichten haben könnte, wird am Beispiel der Vorbereitungsstrafbarkeit im Computerstrafrecht in Kapitel 3 dieser Arbeit ausführlicher behandelt.[181]

Auch wenn vielfach bemängelt wird, dass diese fehlende Orientierung an strafrechtsspezifischen Prinzipien im Strafrecht der Europäischen Union die ohnehin bestehende Gefahr verstärke, dass materielles Strafrecht sowohl als „Vehikel des Zivilrechts“[182] zur effektiven Rechtsdurchsetzung[183] als auch für polizeilich-präventive Ziele zur Gefahrenabwehr zweckentfremdet[184] wird, sind gleichwohl auch im Unionsrecht Grundsätze und Schranken zu finden, die bei der Strafrechtsharmonisierung zu beachten sind. Vor allem relevant sind Bestimmtheitsanforderungen sowie der Grundrechtsschutz.

---

nicht dazu berufene nationale Verfassungsgericht eine solche vornehmen könne; vgl. insoweit BVerfG NJW 2016, 1149 (1159).

177 OLG Bremen NStZ-RR 2015, 322.

178 EuGH, verb. Rs. C-404/15 und C-659/15 PPU, ECLI:EU:C:2016:198 – *Aranyosi u. a.*

179 Siehe insb. EuGH, verb. Rs. C-404/15 und C-659/15 PPU, ECLI:EU:C:2016:198, Rn. 84 ff. – *Aranyosi u. a.*; *Sauer*, NJW 2016, 1134 (1137), sieht durch diese unklare Gemengelage zwischen nationalem und europäischem Recht vor allem die Fachgerichtsbarkeit vor größte Anwendungsschwierigkeiten gestellt.

180 So statt vieler: *Asp. u. a.* (Manifest Kriminalpolitik), ZIS 2009, 697 (706).

181 Siehe unten, Kap. 3 § 12.

182 Siehe *Schmölzer*, ZStW 123 (2011), 709 (720).

183 *Brodowski/Freiling*, Cyberkriminalität, S. 35.

184 So etwa *Heinrich*, ZStW 121 (2009), 94 (123); auch *Heger*, RuP 2012, 88 (94), verweist treffend darauf, dass die EU zuvorderst der Freiheitgewährleistung dienen sollte und daher die Unionspolititk nicht dem Primat der Sicherheit unterzuordnen sei.

Der Bestimmtheitsgrundsatz ist seinem Wesen nach auch im EU-Recht anerkannt. Danach hat eine Norm die Straftaten sowie angedrohten Strafen derart eindeutig zu benennen, dass der Rechtsunterworfene anhand des Wortlauts, gegebenenfalls in Verbindung mit einer gerichtlichen Auslegungspraxis, erkennen kann, wo die Grenzen des Erlaubten verlaufen.[185] Auf Harmonisierungsmaßnahmen ist der Bestimmtheitsgrundsatz freilich nicht direkt übertragbar, ohne dass den mitgliedstaatlichen Legislativorganen gleichzeitig die Entscheidungsspielräume bei der Richtlinienumsetzung entzogen würden.[186] Die Interessen bezüglich eindeutig bestimmter Sekundärrechtsnormen und einer weitreichenden mitgliedstaatlichen Autonomie bei der Umsetzung von EU-Rechtsakten laufen an dieser Stelle mithin gegenläufig zueinander. Die Frage, inwieweit der Bestimmtheitsgrundsatz auf die primärrechtlichen Kompetenznormen anzuwenden ist, da diese das Verhältnis der Europäischen Union gegenüber den Mitgliedstaaten ähnlich einem Staat/Bürger-Verhältnis regeln, wird weiter unten eingehend thematisiert.[187]

Zusätzlich sind materielle Strafrechtsharmonisierungen durch die Europäische Union grundrechtlichen Beschränkungen unterworfen. Damit ist zunächst gemeint, dass die in Art. 5 EUV genannten Organe der Europäischen Union den Garantien der EMRK und der Rechtsprechung des EGMR verpflichtet sind.[188] Diese aus Art. 6 Abs. 3 EUV hervorgehende Beachtungspflicht wird durch Art. 6 Abs. 2 EUV und die damit verbundene Beitrittsklausel der EU zur EMRK noch verstärkt. Ob und wann es tatsächlich zu einem Beitritt kommen wird, ist nach den neuesten Entwicklungen freilich unklar.[189]

Des Weiteren ist das Handeln der Unionsorgane wegen der Grundrechtsintensität strafrechtlicher Eingriffe insbesondere bei Strafrechtsharmonisierungen an der Grundrechtecharta der Europäischen Union (GRC) zu messen. Darin wurden ehemals ungeschriebene strafrechtliche Rechtsgrundsätze kodifiziert[190]

---

[185] Vgl. EuGH, Rs. C-303/05, Slg. 2007 I-03633, Rn. 49 ff. – *Advocaten voor de Wereld VZW/Leden van de Ministeraad*.

[186] Wie hier auch *Geiger*, Strafrechtsharmonisierung, S. 56; demgegenüber allerdings *Asp u. a.* (Manifest Kriminalpolitik), ZIS 2009, 697 (706), die eine Ausweitung des Bestimmtheitsschutzes auf die Sekundärrechtsakte fordern.

[187] Siehe unten, Kap. 2 § 7 B. III.

[188] *Geiger*, Strafrechtsharmonisierung, S. 58 m. w. N.

[189] Im Gutachten des Gerichtshofs 2/13 (Plenum) v. 18.12.2014; abrufbar unter: http://curia.europa.eu/juris/document/document.jsf?text=&docid=160882&pageIndex=0&doclang=DE&mode=req&dir=&occ=first&part=1 (Stand: 07.08.2017), wird angenommen, dass die EU wegen ihrer fehlenden Staatlichkeit nicht Mitglied der EMRK werden und sich damit auch nicht der Rechtsprechung des EGMR unterwerfen könne.

[190] Diese Tendenz betrifft freilich nicht nur Strafrechtsgrundsätze, wie sie *Tridimas*, Principles of EU Law, S. 11 ff. nachzeichnet.

und durch den Vertrag von Lissabon gem. Art. 6 Abs. 1 S. 2 EUV mit primärrechtlichem Status versehen. Von materiell-strafrechtlicher Bedeutung ist insbesondere Art. 49 Abs. 1 GRC (Grundsätze der Gesetzmäßigkeit und der Verhältnismäßigkeit im Zusammenhang mit Straftaten und Strafen).[191] Damit sind das aus dem deutschen Verfassungsrecht bekannte Gesetzlichkeitsprinzip *nullum crimen nulla poena sine lege* sowie das Milderungsgebot mittlerweile auch unionsrechtlich gültig.[192]

2. Struktur des Art. 83 AEUV

Bei der Schaffung und Gewährleistung eines Raums der Freiheit, der Sicherheit und des Rechts achtet die EU u. a. die unterschiedlichen Rechtsordnungen und -traditionen ihrer Mitgliedstaaten (Art. 67 Abs. 1 AEUV). Das Strafrecht nimmt dabei eine besondere Position ein, da es einerseits ein bedeutendes Mittel zur Gewährleistung von Sicherheit ist und andererseits in spezieller Weise ein gewachsenes nationales Rechtsverständnis ausdrückt. Vorgaben für das materielle Strafrecht der EU folgen maßgeblich aus Art. 83 AEUV, der sich aus drei Absätzen zusammensetzt.

a. Art. 83 Abs. 1 AEUV

Der erste Absatz behandelt die Harmonisierung einzelner Kriminalitätsbereiche, deren Straftaten sich durch ihren typischerweise grenzüberschreitenden Charakter und ihre besondere Schwere auszeichnen und bildet den Ausgangspunkt der computerstrafrechtlichen Überlegungen dieser Arbeit. Anhand dieses Absatzes wird die Struktur der strafrechtlichen Legislativkompetenzen der Europäischen Union dargelegt sowie die daran anknüpfende Kritik erörtert.

Die Verantwortlichkeit für die Gewährleistung der Sicherheit verbleibt zwar auch nach dem Vertrag von Lissabon grundsätzlich bei den Mitgliedstaaten

---

[191] Wortlaut des Art. 49 Abs. 1 GRC: „Niemand darf wegen einer Handlung oder Unterlassung verurteilt werden, die zur Zeit ihrer Begehung nach innerstaatlichem oder internationalem Recht nicht strafbar war. Es darf auch keine schwerere Strafe als die zur Zeit der Begehung angedrohte Strafe verhängt werden. Wird nach Begehung einer Straftat durch Gesetz eine mildere Strafe eingeführt, so ist diese zu verhängen."

[192] Nach allgemeiner Auffassung (vgl. statt vieler: *Lenaerts*, EuR 2012, 3, (6 ff.)) kommen den einzelnen Prinzipien durch die Einordnung als Grundrechte bzw. Grundsätze Aufgaben zu, die gem. Art. 52 GRC auch unterschiedliche Auslegungsbezugspunkte nach sich ziehen. Da vorliegend lediglich ein genereller Rahmen der europäischen Strafrechtsprinzipien aufgezeigt werden soll, ist eine vertiefte Auseinandersetzung mit diesen Unterschieden an dieser Stelle weder geboten noch möglich. Es wird auf die umfassende Darstellung und Analyse bei *Schaut*, Europäische Strafrechtsprinzipien, S. 50 ff. verwiesen.

selbst, jedoch kann die grenzüberschreitende Dimension von Straftaten dazu führen, dass zumindest gemeinsame Untergrenzen notwendig sind oder werden.[193]

Erstens ist es die Intention solcher Strafuntergrenzen, „sichere Häfen" zu vermeiden, sodass die Ausübung krimineller Aktivitäten aus einzelnen Mitgliedstaaten, mit einem niedrigeren Strafbarkeitsniveau als in der restlichen Union, heraus verhindert wird.[194] Zweitens sollen „Trittbrettfahrerwirkungen" unterbunden werden, bei denen einzelne Mitgliedstaaten durch geringere Strafbarkeitsniveaus Vorteile erzielen, indem sie auf diesem Wege Unternehmen anlocken und so die Wettbewerbsgleichheit stören.[195] Drittens ist die Verfolgung grenzüberschreitender Kriminalität vielfach nur dann möglich, wenn die mitgliedstaatlichen Strafverfolgungsbehörden international zusammenarbeiten. Die Zusammenarbeit erfordert regelmäßig eine beiderseitige Strafbarkeit der betreffenden Verhaltensweisen oder eine gegenseitige Anerkennung der betroffenen Staaten, sodass auch für diesen Aspekt der Kriminalitätsbekämpfung eine Strafbarkeitsangleichung, die mit gemeinsamen Strafuntergrenzen einhergeht, förderlich ist.[196] Dabei kann sich eine grenzüberschreitende Dimension auch schlicht aus der Tatsache ergeben, dass sich eine Straftat gegen grundlegende Werte der Europäischen Union (Art. 2 EUV) richtet und diese es daher nicht hinnehmen kann, dass derartige Verhaltensweisen in einem Mitgliedstaat straflos bleiben.[197]

aa. Art. 83 Abs. 1 UAbs. 1 AEUV

Art. 83 Abs. 1 UAbs. 1 AEUV ermächtigt die Europäische Union dazu, „durch Richtlinien Mindestvorschriften zur Festlegung von Straftaten und Strafen in Bereichen besonders schwerer Kriminalität fest[zu]legen, die aufgrund der Art oder der Auswirkungen der Straftaten oder aufgrund einer besonderen Notwendigkeit, sie auf einer gemeinsamen Grundlage zu bekämpfen, eine grenzüberschreitende Dimension haben".

---

[193] *Böse*, in: Schwarze (Hrsg.), Art. 83 AEUV Rn. 2.

[194] *Vogel/Eisele*, in: Grabitz/Hilf/Nettesheim (Hrsg.), Art. 83 AEUV Rn. 10.

[195] *Meyer*, in: von der Groeben/Schwarze/Hatje (Hrsg.), Art. 83 AEUV Rn. 3; siehe insb. auch *Satzger*, Europäisierung des Strafrechts, S. 429 m. w. N., der auf den sog. Delaware-Effekt Bezug nimmt, welcher den Umstand beschreibt, dass ein Staat durch ein liberales Steuer- und Wirtschaftsrecht die Ansiedlung von Unternehmen vorantreibt und sich auf diese Weise einen unfairen Wettbewerbsvorteil sichert.

[196] *Satzger*, in: Streinz (Hrsg.), Art. 83 AEUV Rn. 3, der die dienende Funktion der materiellen Harmonisierung gegenüber dem Prinzip der gegenseitigen Anerkennung hervorhebt; siehe auch *Vogel*, in: Böse (Hrsg.), EnzEuR Bd. 9, § 7 Rn. 24.

[197] *Meyer*, in: von der Groeben/Schwarze/Hatje (Hrsg.), Art. 83 AEUV Rn. 3; *Vogel*, in: Böse (Hrsg.), EnzEuR Bd. 9, § 7 Rn. 10.

Richtlinien nach Art. 288 Abs. 3 AEUV sind die einzige Handlungsform, die Art. 83 AEUV zur Strafrechtsharmonisierung zur Verfügung stellt.[198] Diese haben in den Mitgliedstaaten keine unmittelbare Geltung, sondern bedürfen der Umsetzung in nationales Recht. Zwar ist das Ziel der Umsetzung verbindlich, jedoch sind die Mitgliedstaaten in der Wahl von Form und Mittel der Umsetzung anhand des jeweiligen (Verfassungs-)Rechts frei.[199] Aus sich selbst heraus vermögen Richtlinien eine individuelle Strafbarkeit nicht zu begründen, nach ihrer Umsetzung in nationales Strafrecht sind sie jedoch im Rahmen der richtlinienkonformen Auslegung des nationalen Strafgesetzes bedeutsam. Während dadurch unstreitig eine Strafbarkeitseinschränkung erreicht werden kann,[200] ist eine Strafbarkeitserweiterung im Wege richtlinienkonformer Auslegung des nationalen Strafgesetzes nach der Rechtsprechung des EuGH nur zulässig, wenn dem der Wortlaut der nationalen Strafvorschrift nicht entgegensteht und die Richtlinie in diesem Punkt hinreichend bestimmt gefasst ist.[201]

Mindestvorschriften über Straftaten beschreiben diejenigen Verhaltensweisen, die mindestens unter Strafe gestellt werden müssen, während Mindestvorschriften über Strafen festlegen, welche Strafen mindestens anzudrohen oder zu verhängen sind.[202] Beachtenswert ist zusätzlich, dass eine „limitierende Strafrechtsangleichung“, also etwa Vorschriften über Höchststrafen, weder vom Wortlaut noch vom Sinn und Zweck des Art. 83 AEUV gedeckt sind, und daher eine Limitierung lediglich über die Grund- und Menschenrechte im Unions- und Völkerrecht sichergestellt ist.[203]

Im Lichte des unionsrechtlichen Bestimmtheitsgrundsatzes aus Art. 49 Abs. 1 S. 1 GRC und des auch unionsrechtlich anerkannten Schuldprinzips müssen die Tatbestandsmerkmale sowohl in objektiver als auch in subjektiver Hinsicht hinreichend bestimmt sein und mithin einen vollständigen Tatbestand ergeben.[204]

---

[198] Zum Gesetzgebungsverfahren siehe auch *Nettesheim*, in: Grabitz/Hilf/ders. (Hrsg.), 57. EL Aug. 2015, Art. 288 AEUV Rn. 108.

[199] Statt aller: *Kotzur*, in: Geiger/Khan/ders. (Hrsg.), § 288 AEUV Rn. 12.

[200] *Vogel*, in: Böse (Hrsg.), EnzEuR Bd. 9, § 7 Rn. 28.

[201] EuGH, verb. Rs. C-74/95 und C-129/95, Slg. 1996, I-6609 Rn. 24 f. und 31; siehe auch *Hecker*, Europäisches Strafrecht, Kap. 10 Rn. 61 ff.; *Satzger*, Internationales und Europäisches Strafrecht, § 9 Rn. 91.

[202] *Vogel/Eisele*, in: Grabitz/Hilf/Nettesheim (Hrsg.), 57. EL Aug. 2015, Art. 83 AEUV Rn. 32.

[203] Vgl. *Böse*, in: Schwarze (Hrsg.), Art. 83 AEUV Rn. 17; *Satzger*, in: Streinz (Hrsg.), Art. 83 AEUV Rn. 2; *Vogel/Eisele*, in: Grabitz/Hilf/Nettesheim (Hrsg.), 57. EL Aug. 2015, Art. 83 AEUV Rn. 21, 32.

[204] *Vogel/Eisele*, in: Grabitz/Hilf/Nettesheim (Hrsg.), 57. EL Aug. 2015, Art. 83 AEUV Rn. 35; während das BVerfGE 123, 267 (413) davon ausgeht, dass es auch möglich ist, lediglich Tatbestandvarianten in den Richtlinientext aufzunehmen.

Bei der Festlegung von Mindestvorschriften für Strafen kann der Unionsgesetzgeber grundsätzlich auf sämtliche „strafrechtliche[n] Sanktionen und Rechtsfolgen“, und somit auch auf Nebenstrafen oder -rechtsfolgen, zurückgreifen, beschränkt sich in der Praxis allerdings bisher auf die unionsweit anerkannten Freiheits- und Geldstrafen.[205] Eine geringe Regelungsdichte stellt in diesem Zuge die Vorgabe dar, dass „wirksame, verhältnismäßige und abschreckende Strafen bzw. strafrechtliche Sanktionen vorzusehen sind“,[206] während eine höhere Vorgabenstufe die sog. Mindest-Höchststrafen einnehmen, bei denen eine bestimmte Straftat zumindest mit einer bestimmten Höchststrafe zu bedrohen ist.[207] Vom Äquivalent sog. Mindest-Mindeststrafen hat der Unionsgesetzgeber bisher abgesehen, da solche besonders stark in die mitgliedstaatlichen Strafrechtsordnungen eingreifen würden.[208]

Dem Unionsgesetzgeber sind Harmonisierungsmaßnahmen über Art. 83 Abs. 1 AEUV ausschließlich in Bereichen besonders schwerer Kriminalität mit grenzüberschreitender Dimension möglich. Als Ausfluss der Grundsätze der Subsidiarität und der Verhältnismäßigkeit, die aus verfassungsrechtlicher Sicht überhaupt erst die Übertragung von Hoheitsrechten rechtfertigen, müssen jene Voraussetzungen kumulativ vorliegen.[209] Hinsichtlich der Definitionen und einer eingehenden Auseinandersetzung mit den beiden Voraussetzungen sei an dieser Stelle auf den Abschnitt zur Auslegung des Begriffs der Computerkriminalität verwiesen.[210]

bb. Art. 83 Abs. 1 UAbs. 2 AEUV

Art. 83 Abs. 1 UAbs. 2 AEUV nennt diejenigen Kriminalitätsbereiche, welche die Voraussetzungen „besonders schwerer Kriminalität“ und „grenzüberschreitende[r] Dimension“ erfüllen: „Terrorismus, Menschenhandel und sexuelle Ausbeutung von Frauen und Kindern, illegaler Drogenhandel, illegaler Waffenhan-

---

[205] *Böse*, in: Schwarze (Hrsg.), Art. 83 AEUV Rn. 20; *Vogel/Eisele*, in: Grabitz/Hilf/Nettesheim, 57. EL Aug. 2015, Art. 83 AEUV Rn. 37.

[206] Beispiele dafür finden sich in Art. 3 Abs. 1 des Rahmenbeschlusses 2002/629/JI des Rats v. 19.7.2002 zur Bekämpfung des Menschenhandels, ABl. L 203 v. 1.8.2003, S. 1 und in Art. 5 Abs. 1 des Rahmenbeschlusses 2004/68/JI des Rats v. 22.12.2003 zur Bekämpfung der sexuellen Ausbeutung von Kindern und der Kinderpornografie, ABl. L 13 v. 20.1.2004, S. 44.

[207] *Hecker*, Europäisches Strafrecht, Kap. 11 Rn. 7; *Satzger*, Internationales und Europäisches Strafrecht, § 9 Rn. 45; *Vogel/Eisele*, in: Grabitz/Hilf/Nettesheim (Hrsg.), 57. EL Aug. 2015, Art. 83 AEUV Rn. 38.

[208] *Vogel/Eisele*, in: Grabitz/Hilf/Nettesheim (Hrsg.), 57. EL Aug. 2015, Art. 83 AEUV Rn. 38.

[209] BVerfGE 123, 267 (410); *Meyer*, in: von der Groeben/Schwarze/Hatje (Hrsg.), Art. 83 AEUV Rn. 8; *Satzger*, in: Streinz (Hrsg.), Art. 83 AEUV Rn. 9.

[210] Siehe unten, Kap. 2 § 7 A.

del, Geldwäsche, Korruption, Fälschung von Zahlungsmitteln, Computerkriminalität und organisierte Kriminalität". Größtenteils handelt es sich hierbei um „moderne Kriminalität", deren Modernität sich entweder aus dem kurzfristigen Entstehen oder der erstmaligen Kriminalisierung des Bereichs (Computerkriminalität, Geldwäsche) oder der gestiegenen internationalen Bedeutung durch eine fortschreitende Globalisierung (Menschenhandel, Korruption) ergibt.[211]

Im Gegensatz zur Vorgängerregelung des Art. 31 Abs. 1 lit. e EUV a. F. ist die Liste des Art. 83 Abs. 1 UAbs. 2 AEUV abschließend und kann lediglich nach Art. 83 Abs. 1 UAbs. 3 AEUV erweitert werden. Somit liegt im Grundsatz in der Neufassung eine Beschränkung gegenüber dem Art. 31 Abs. 1 lit. e EUV a. F. vor, da im alten Recht sowohl nach der vorherrschenden Unionspraxis als auch der herrschenden Literaturansicht jede Form der Kriminalität grundsätzlich harmonisiert werden durfte.[212] Dem Wortlaut entsprechend, findet eine weitere Prüfung der einzelnen Kriminalitätsbereiche dahin gehend, ob sie tatsächlich die Voraussetzungen der besonderen Schwere und der grenzüberschreitenden Dimension erfüllen, nicht mehr statt.[213] Da die Kompetenzvorschrift des Art. 83 AEUV nicht den strafrechtlichen Bestimmtheitsanforderungen genügen muss,[214] wird ihre Auslegung, und damit eine Bestimmung des Inhalts der Kriminalitätsbereiche, unter Berücksichtigung der völker- und unionsrechtlichen Grundprinzipien vorgenommen.[215] Hinsichtlich dieses zentralen Punkts der Auslegungsmethodik im Mehrebenensystem zwischen Europäischer Union und Mitgliedstaaten sei auf die Ausführungen im Rahmen des zweiten Kapitels verwiesen.[216]

---

[211] *Tiedemann*, Wirtschaftsstrafrecht BT, Rn. 40; *Vogel/Eisele*, in: Grabitz/Hilf/Nettesheim (Hrsg.), Art. 83 AEUV Rn. 49.

[212] Siehe insb. *Heger*, in: Giegerich (Hrsg.), Herausforderungen und Perspektiven der EU, S. 157 (180) sowie *ders.*, ZIS 2009, 406 (412), der darstellt, dass es sich nach h. A. beim engen Wortlaut des Art. 31 Abs. 1 lit. e EUV a. F. um ein Redaktionsversehen gehandelt habe; vgl. auch *Satzger*, in: Streinz (Hrsg.), Art. 83 AEUV Rn. 11; *Vogel/Eisele*, in: Grabitz/Hilf/Nettesheim (Hrsg.), 57. EL Aug. 2015, Art. 83 AEUV Rn. 48.

[213] *Böse*, in: Schwarze (Hrsg.), Art. 83 AEUV Rn. 8; *Vogel/Eisele*, in: Grabitz/Hilf/Nettesheim (Hrsg.), 57. EL Aug. 2015, Art. 83 AEUV Rn. 48; *Zöller*, in: FS Schenke (2011), S. 579 (587); a. A. *Satzger*, in: Streinz (Hrsg.), Art. 83 AEUV Rn. 10.

[214] *Ambos/Rackow*, ZIS 2009, 397 (402); *Vogel/Eisele*, in: Grabitz/Hilf/Nettesheim (Hrsg.), 57. EL Aug. 2015, Art. 83 AEUV Rn. 51; siehe auch unten, Kap. 2 § 7 B. III.

[215] *Böse*, in: Schwarze (Hrsg.), Art. 83 AEUV Rn. 9; *Vogel/Eisele*, in: Grabitz/Hilf/Nettesheim (Hrsg.), 57. EL Aug. 2015, Art. 83 AEUV Rn. 52.

[216] Siehe unten, Kap. 2 § 7 C.

cc. Art. 83 Abs. 1 UAbs. 3 AEUV

Art. 83 Abs. 1 UAbs. 3 AEUV stellt klar, dass diese Aufzählung durch einstimmigen Beschluss des Rats nach Zustimmung des Europäischen Parlaments erweitert werden kann, indem „je nach Entwicklung der Kriminalität […] andere Kriminalitätsbereiche bestimmt werden, die die Kriterien dieses Absatzes erfüllen“. Zumeist wird angenommen, dass diese genannte Kriminalitätsentwicklung nicht lediglich behauptet werden dürfe, sondern auch tatsächlich statistisch nachgewiesen werden müsse.[217] Dabei können nur solche Kriminalitätsbereiche in den Katalog des Art. 83 Abs. 1 UAbs. 2 AEUV aufgenommen werden, die die Voraussetzungen der besonderen Schwere und grenzüberschreitenden Dimension erfüllen. In Anbetracht des äußerst umfangreichen Katalogs fällt es nicht leicht, sich viele weitere Kriminalitätsbereiche vorzustellen, die den Kriterien entsprechen.[218] Obgleich diesen potenziell neu aufzunehmenden Bereichen nicht abzuverlangen ist, dass es sich um gänzlich neue Kriminalitätserscheinungen handelt,[219] wird man wohl zumindest auf substanzielle Entwicklungen und gewisse neue Phänomene bestehen müssen, die der Rat im Rahmen eines gewissen Einschätzungsspielraums zu bewerten hat.

b. Art. 83 Abs. 2 AEUV

Im zweiten Absatz wird die sog. strafrechtliche Annexkompetenz festgelegt. So können auf anderen Gebieten erfolgte Harmonisierungsmaßnahmen strafrechtlich flankiert werden, soweit dies für die wirksame Durchführung der Politik der Union auf diesem anderen Gebiet „unerlässlich“ ist. Dabei wird zur Rechtfertigung einer solchen Annexkompetenz angenommen, dass eine effektive Unionspolitik nur dann stattfinden kann, wenn durch mitgliedstaatliches Strafrecht sichergestellt ist, dass Verstöße gegen das Recht der Union mit abschreckenden, effektiven und verhältnismäßigen Sanktionen belegt werden.[220] Eine solche strafrechtliche Annexkompetenz hatte der EuGH bereits vor Inkrafttreten des Art. 83 Abs. 2 AEUV für die Europäische Gemeinschaft angenommen.[221] Durch die ausdrückliche Übernahme dieser Kompetenz in das Primärrecht und die darin verankerte Akzessorietät bezüglich Harmonisierungskompetenzen auf anderen Politikfeldern wurden den strafrechtlichen Möglichkeiten

---

[217] *Calliess*, Die neue EU, S. 471; *Suhr*, in: Calliess/Ruffert (Hrsg.), Art. 83 AEUV Rn. 15; *Vogel/Eisele*, in: Grabitz/Hilf/Nettesheim (Hrsg.), 57. EL Aug. 2015, Art. 83 AEUV Rn. 66.

[218] *Folz*, ZIS 2009, 427 (430); *Mansdörfer*, HRRS 2010, 11 (16 f.).

[219] *Satzger*, in: Streinz (Hrsg.), Art. 83 AEUV Rn. 21.

[220] *Böse*, in: Schwarze (Hrsg.), Art. 83 AEUV Rn. 25.

[221] EuGH, Rs. C-176/03, Slg. 2005, I-07879 – *Umweltstrafrecht*; Rs. C-308/06, Slg. 2008, I-04057 – *Meeresverschmutzung*; vgl. auch *Böse*, in: Schwarze (Hrsg.), Art. 83 AEUV Rn. 1.

des Art. 83 Abs. 2 AEUV direkt Grenzen gesetzt.[222] Die Notwendigkeit einer Annexkompetenz, um Unionsrecht effektiv durchsetzen zu können, wurde nie ernsthaft infrage gestellt. Bevor sie allerdings in Art. 83 Abs. 2 AEUV auch tatsächlich kodifiziert worden ist, konnte lediglich auf die allgemeine Loyalitätspflicht des Art. 4 Abs. 3 EUV zurückgegriffen werden.[223] Die explizite Aufnahme einer ohnehin anerkannten und praktizierten Kompetenz der EU ist daher insbesondere aus Gründen der Verständlichkeit des EU-Rechts zu begrüßen.

Nichtsdestotrotz wird diese Annexkompetenz in Rechtsprechung und Literatur kritisiert. Zum einen wird befürchtet, dass Art. 83 Abs. 2 AEUV eine „uferlose bzw. grenzenlose" Ermächtigung der Europäischen Union zur Strafrechtsharmonisierung bedeute.[224] Zum anderen wird bemängelt, dass das Strafrecht durch die Annexkompetenz als bloßer „Durchsetzungsmechanismus" missbraucht werde.[225]

Der strafrechtliche Auftrag zum Rechtsgüterschutz könnte untergraben werden, falls nicht mehr im Sinne des *Ultima-Ratio*-Grundsatzes nur dasjenige Verhalten mit Strafe bedroht wird, das gegen das sog. sozial-ethische Minimum einer Gesellschaft verstößt.[226] Es steht zu befürchten, dass sämtlichen Unionsrechtsakten strafrechtliche Flankierungsmaßnahmen hinzugefügt werden. Beispielsweise könnte auf diese Weise EU-rechtliche Sozialgesetzgebung mit strafrechtlichen Mitteln „abgesichert" werden. Dies könnte wiederum eine Umgehung der hohen Anforderungen des Art. 83 Abs. 1 AEUV (besonders schwere Kriminalität mit typischerweise grenzüberschreitendem Charakter) darstellen.

Dieser Kritik wird entgegengehalten, dass eine Strafnorm nur dann gerechtfertigt sei, wenn nach Maßgabe des Verhältnismäßigkeitsprinzips ein Strafzweck bestehe, und erst dann könne die Strafe als Mittel oder Instrument zur Zweckerreichung eingesetzt werden.[227] Die mit den Unionspolitiken verfolgten Ziele seien letztlich als Bezugspunkte einer solchen Verhältnismäßigkeitsprüfung durchaus geeignet.[228] Außerdem werde durch die akzessorische, also nachfolgende, Anknüpfung an „außerstrafrechtliche" Harmonisierungsakte sichergestellt, dass sich zunächst andere Mittel zur Durchsetzung des Unionsrechts

---

[222] *Böse*, in: Schwarze (Hrsg.), Art. 83 AEUV Rn. 25.

[223] Zur allg. Loyalitätspflicht siehe EuGH, Rs. C-68/88, Slg. 1989, 2985, Rn. 24 f. – *Griechischer Mais*.

[224] BVerfGE 123, 267 (411); *Ambos/Rackow*, ZIS 2009, 397 (401); *Walter*, ZStW 117 (2005), 912 (928).

[225] *Satzger*, in: Streinz (Hrsg.), Art. 83 AEUV Rn. 26.

[226] Siehe zur Thematik der Funktionen und Grundprinzipien des Strafrechts vor allem unten, Kap. 3 § 12 C.

[227] *Vogel/Eisele*, in: Grabitz/Hilf/Nettesheim (Hrsg.), 57. EL Aug. 2015, Art. 83 AEUV Rn. 75.

[228] *Böse*, in: Schwarze (Hrsg.), Art. 83 AEUV Rn. 25.

als nicht ausreichend erwiesen haben[229] oder zumindest bei Inanspruchnahme der Annexkompetenz die Grundsätze von Subsidiarität und Verhältnismäßigkeit derartig Beachtung finden, dass die Unerlässlichkeit einer strafrechtlichen Regelung rechtlich und tatsächlich explizit begründet wird.[230]

Unter Beachtung der von den EU-Organen praktizierten und am *effet utile* orientierten Auslegung des Unionsrechts,[231] die auch vom Bundesverfassungsgericht grundsätzlich anerkannt ist,[232] besteht durchaus die Gefahr, dass die Annexkompetenz des Art. 83 Abs. 2 AEUV zur strafrechtlichen Harmonisierung von Rechtsbereichen genutzt wird, die nicht den Erfordernissen des Art. 83 Abs. 1 AEUV entsprechen und lediglich der Flankierung von außerstrafrechtlichen Bereichen des EU-Rechts dienen. Diese Entwicklung durch die Aufstellung besonderer Erfordernisse an den empirischen Nachweis der Unerlässlichkeit oder die Erfüllung anderer, vor allem der deutschen Rechtstradition entspringender Grundsätze verhindern zu wollen, erscheint allerdings wenig zielführend. Der EuGH hat mehrfach betont und bewiesen, dass er strafrechtliche Kompetenznormen dynamisch und extensiv auslegt und auch nicht strafrechtliche Ermächtigungsgrundlagen zur strafrechtlichen Kompetenzbegründung heranzuziehen gedenkt.[233] Zielführender hingegen ist es, die Beachtung der EU-rechtlichen Prinzipien der Subsidiarität und der Verhältnismäßigkeit zu fordern, die dem Merkmal der Unerlässlichkeit mindestens implizit zu entnehmen sind[234] und die darüber hinaus auch auf Kompetenzbegründungs- bzw.

---

[229] BVerfGE 123, 267 (412); *Suhr*, in: Calliess/Ruffert (Hrsg.), Art. 83 AEUV Rn. 25; a. A. *Reinbacher*, Strafrecht im Mehrebenensystem, S. 481; *Safferling*, Internationales Strafrecht, § 10 Rn. 58; *Vogel/Eisele*, in: Grabitz/Hilf/Nettesheim (Hrsg.), 57. EL Aug. 2015, Art. 83 AEUV Rn. 77 ff., die dem EU-Gesetzgeber, analog dem nationalen Gesetzgeber, eine Einschätzungsprärogative hinsichtlich der Unerlässlichkeit einer Annexkriminalisierung zugestehen.

[230] *Böse*, in: Schwarze (Hrsg.), Art. 83 AEUV Rn. 26. Eine praktische Umsetzung dieser Anforderungen findet bislang freilich nicht statt, worauf *Asp u. a.* (Manifest Kriminalpolitik), ZIS 2009, 697 (699) hinweisen.

[231] *Safferling*, Internationales Strafrecht, § 10 Rn. 57; *Vogel*, in: Ambos (Hrsg.), Europäisches Strafrecht post-Lissabon, S. 41 (43).

[232] *Reinbacher*, Strafrecht im Mehrebenensystem, S. 481.

[233] *Vogel*, in: Ambos (Hrsg.), Europäisches Strafrecht post-Lissabon, S. 41 (43) unter Bezugnahme auf EuGH, Rs. C-176/03, Slg. 2005, I-7879 – *Kommission/Rat*.

[234] Ähnlich auch *Hecker*, Europäisches Strafrecht, Kap. 8 Rn. 48; *Reinbacher*, Strafrecht im Mehrebenensystem, S. 479; sogar die EU-Kommission brachte im Zusammenhang mit der Entscheidung zur Meeresverschmutzung vor, dass die Begriffe „unerlässlich“ (damals noch bezogen auf die Rechtsprechung des EuGH, mittlerweile ist der Begriff allerdings Merkmal des Art. 83 Abs. 2 AEUV, der als Kodifizierung der vorangegangenen „Annex-Rechtsprechung“ des EuGH zu verstehen ist) und „erforderlich“ (Art. 29 EUV a. F.) bedeutungsidentisch seien, vgl. insoweit EuGH, Rs. C-440/05, Slg. 2007, I-9150, Rn. 38 – *Kommission/Rat*.

-ausübungsebene im Wege der Nichtigkeitsklage nach Art. 263 AEUV justiziabel sind.[235]

Sollten darüber hinaus noch grundlegende Aspekte einer nationalen Strafrechtsordnung von auf der Annexkompetenz beruhenden Strafrechtsakten betroffen sein, ist die Auslösung des sog. Notbremsemechanismus nach Art. 83 Abs. 3 AEUV durch den jeweiligen Mitgliedstaat denkbar.

c. Art. 83 Abs. 3 AEUV

Der dritte Absatz schließlich statuiert den sog. Notbremsemechanismus. Danach kann sich ein Mitglied des Rats im Rahmen eines Gesetzgebungsverfahrens nach Art. 83 Abs. 1 oder Abs. 2 AEUV darauf berufen, dass die Maßnahme grundlegende Aspekte seiner nationalen Strafrechtsordnung berühre, und beantragen, dass der Europäische Rat mit der Sache befasst wird.[236]

C. Europäische Union und Computerkriminalität

Neben dem Europarat hat sich auch die Europäische Union den Herausforderungen auf dem Gebiet der Computerkriminalität angenommen. Ihre Tätigkeiten reichen dabei von der Betonung der Relevanz dieses Themenfelds in der Unionspolitik[237] über die Ausarbeitung oder Unterstützung von Studien[238] sowie die Veröffentlichung von Kommissions-Mitteilungen[239] bis hin zur Verrechtlichung der zuvor genannten Aspekte im Wege von Rahmenbeschlüssen[240] bzw. von Richtlinien.[241]

I. Unionspolitische Programmatik

Bereits gegen Ende der 1990er-Jahre gab es in der Europäischen Union erste vorsichtige Ansätze, eine Harmonisierung im Bereich der Computerkriminalität als Bekämpfungsmethode anzusehen. Der *Aktionsplan des Rates und der Kommission zur bestmöglichen Umsetzung der Bestimmungen des Amsterdamer Vertrags über den Aufbau eines Raumes der Freiheit, der Sicherheit und*

---

[235] Bezüglich der Überprüfung von Rechtsbegriffen des Unionsrechts durch den EuGH siehe unten, Kap. 3 § 12 D. II.
[236] Siehe insbesondere unten, Kap. 3 § 12 D. II. 2.
[237] Siehe unten, Kap. 1 § 2 C. I.
[238] Siehe unten, Kap. 1 § 2 C. II.
[239] Siehe unten, Kap. 1 § 2 C. III.
[240] Siehe unten, Kap. 1 § 2 C. IV.
[241] Siehe unten, Kap. 1 § 2 C. V.

des Rechts vom 3.12.1998[242] zählt in C. III. a) die „Internet-Kriminalität" als eine Kriminalitätsform auf, die einer „Festlegung von Mindestvorschriften über die Tatbestandsmerkmale einer strafbaren Handlung und die dafür geltenden Strafen" bedürfen könnte. Dabei seien parallel laufende Arbeiten in internationalen Organisationen wie dem Europarat zu berücksichtigen.

Der Europäische Rat stellt alle fünf Jahre einen Plan zur Umsetzung des mit dem Vertrag von Amsterdam als Unionsziel eingeführten Raums der Freiheit, der Sicherheit und des Rechts in der Europäischen Union auf. Zurzeit gilt das sog. Stockholmer Programm[243], das auf dem Tampere-Programm[244] und dem Haager Programm[245] aufbaut. In Kapitel 4 („Ein Europa, das schützt") geht der Plan auf Schwerpunktfelder der inneren Sicherheit ein. Unter 4.4.4 wird die Cyberkriminalität zu einer zu bewältigenden Herausforderung für ein sichereres Europa erklärt. Nach einer allgemeinen Bestandsaufnahme einer mit fortschreitender Technisierung des Alltags einhergehenden Kriminalprävention und Ermittlungstätigkeit gibt der Europäische Rat Ziele aus und fordert Kommission und Mitgliedstaaten zum Handeln auf. So wird die Kommission ersucht, Maßnahmen zur Verbesserung der Kollaboration zwischen privatem und öffentlichem Sektor zu ergreifen und den Rechtsrahmen für Ermittlungen zur Cyberkriminalität und bezüglich des anzuwendenden Rechts im Cyberraum zu präzisieren. Die Mitgliedstaaten hingegen werden aufgerufen, die justizielle Zusammenarbeit bei der Bekämpfung von Cyberkriminalität zu intensivieren. Schließlich wird es Europol auferlegt, regelmäßig Erhebungen zur Entwicklung der Cyberkriminalität durchzuführen.

II. Studien

Anfang 1998 hat *Sieber* im Auftrag der Europäischen Kommission die sog. COMCRIME-Studie („Legal Aspects of Computer-Related Crime in the Information Society") erarbeitet und veröffentlicht.[246] Die COMCRIME-Studie stellt aktuelle Informationen zum materiellen und prozessualen Computerstrafrecht

---

[242] ABl. C 19 v. 23.1.1999, S. 1.

[243] Informationen der Organe, Einrichtungen und sonstigen Stellen der Europäischen Union durch den Europäischen Rat: Das Stockholmer Programm – Ein offenes und sicheres Europa im Dienste und zum Schutz der Bürger, ABl. C 115 v. 4.5.2010, S. 1.

[244] Europäischer Rat (Tampere) v. 15./16.10.1999, in: von der Groeben (Hrsg.), Handbuch des Europäischen Rechts, Justizielle Zusammenarbeit in Strafsachen/Polizeiliche Zusammenarbeit, 423. Lieferung – Februar 2002, I A 14/1.3, S. 1.

[245] Haager Programm zur Stärkung von Freiheit, Sicherheit und Recht in der Europäischen Union, ABl. C 53 v. 3.3.2005, S. 1.

[246] *Sieber*, COMCRIME-Studie; abrufbar unter: http://www.edc.uoc.gr/~panas/PATRA/sieber.pdf (Stand: 07.08.2017).

zusammen und liefert Alternativvorschläge für ein zukünftiges Vorgehen. Zunächst mahnt *Sieber* an, dass sämtliche Ansätze zur Bekämpfung der Computerkriminalität international gedacht werden müssten, um *computer crime havens* zu verhindern. Zweitens seien umfassende Maßnahmen zu ergreifen, die auch und insbesondere nicht juristische Mittel, wie etwa technologische, bildungsnahe und industriell-selbstregulierende Mittel, einbezögen. Drittens solle es sich immer um daten- und informationsspezifische Maßnahmen handeln, die die rechtlichen Besonderheiten der Nicht-Körperlichkeit eines Datums berücksichtigten.[247] Als weiteren wichtigen Aspekt macht *Sieber* die koordinierte Zusammenarbeit aller mit der Bekämpfung von Computerkriminalität befassten internationalen Organisationen aus, um überflüssige Dopplungen zu vermeiden. Wichtigste Beteiligte seien die EU, der Europarat, die OECD, die G8, Interpol und die Vereinten Nationen.[248]

III. Mitteilungen

Ebenfalls bereits vor ca. 20 Jahren griff die Europäische Kommission sowohl in einem Grünbuch[249] als auch in einer taggleich erschienenen Mitteilung[250] die Problematik von Straftaten im Internet und deren Bekämpfung auf. Darin wird zunächst der Jugendschutz als Ziel ausgegeben. Daneben wird deutlich gemacht, dass zwischen der Sicherung des freien Informationsflusses sowie dem Schutz des öffentlichen Interesses abgewogen werden müsse.[251]

Mit der Mittelung zur Schaffung einer sicheren Informationsgesellschaft[252] werden dann Legislativvorschläge zur materiellen Strafrechtsharmonisierung im Bereich der Hightechkriminalität sowie zur verstärkten Zusammenarbeit der Mitgliedstaaten unter Koordination der Europäischen Union in Aussicht gestellt. Ein Jahr später nimmt die Mitteilung zur Sicherheit der Netze[253] vor allem

[247] Siehe insb. zu diesen drei Aspekten *Sieber*, COMCRIME-Studie, S. 5.

[248] *Sieber*, COMCRIME-Studie, S. 8.

[249] KOM (1996) 483 endg.: Grünbuch über den Jugendschutz und den Schutz der Menschenwürde in den audio-visuellen und den Informationsmedien.

[250] KOM (1996) 487 endg.: Mitteilung der Kommission an den Rat, das Europäische Parlament, den Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen: Illegale und schädigende Inhalte im Internet.

[251] KOM (1996) 487 endg., S. 5.

[252] KOM (2000) 890 endg.: Mitteilung der Kommission an den Rat, das Europäische Parlament, den Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen: Schaffung einer sichereren Informationsgesellschaft durch Verbesserung der Sicherheit von Informationsinfrastrukturen und Bekämpfung der Computerkriminalität.

[253] KOM (2001) 298 endg.: Mitteilung der Kommission an den Rat, das Europäische Parlament, den Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen: Sicherheit der Netze und Informationen: Vorschlag für einen europäischen Politikansatz.

die europäische Netz- und Informationssicherheit sowie den Datenschutz in den Fokus. Während die Förderung des technischen Fortschritts besonders hervorgehoben wurde, nahm das materielle Strafrecht noch eine untergeordnete Rolle ein.[254]

Die Mitteilung zur Bekämpfung der Internetkriminalität[255] präzisierte diese Ansätze und nimmt eine erste vorsichtige Begriffsbestimmung der Internetkriminalität vor. Bemerkenswert an dieser Mitteilung ist, dass die Kommission eine materielle Harmonisierung des Computerstrafrechts für unangebracht hielt, weil noch zu viele unterschiedliche Delikte in diesen Bereich fallen würden.[256]

In ihrer Mitteilung zum Schutz kritischer Informationsinfrastrukturen[257] mahnt die Europäische Kommission Maßnahmen zur Verbesserung der europäischen Abwehrbereitschaft an, da insbesondere Informations- und Kommunikationsinfrastrukturen für die europäische Wirtschaft und Gesellschaft unverzichtbar seien. Sie unterstützten einerseits herkömmliche kritische Infrastrukturen teilweise grundlegend und stellten andererseits selbst eine kritische Infrastruktur dar. In der Digitalen Agenda[258] wurden daraufhin mit Ausblick auf das Jahr 2020 Ziele formuliert, um die Europäische Union als Wirtschaftsgemeinschaft nachhaltig zu stärken. Der Ausbau digitaler Technologien und die Vernetzung von Wirtschaftssektoren mit den Verbrauchern seien dabei wesentliche Faktoren.[259] Gleichzeitig komme der Bekämpfung von Computerkriminalität eine Schlüsselrolle für eine erfolgreiche Digitalisierung des europäischen Wirtschafts- und Sozialgefüges zu. Denn auf der einen Seite seien nur sichere und widerstandsfähige Produkte international marktfähig, auf der anderen Seite könne erst dann von den vielfältigen Angeboten einer digitalen europäischen Wirtschaft und Gesellschaft profitiert werden, wenn die Bürger Europas das nötige Vertrauen in die Sicherheit ihrer Daten und der genutzten Anwendungen

---

[254] Vgl. auch *Hilgendorf*, in: Internet-Recht und Strafrecht, 2005, S. 263 f.

[255] KOM (2007) 267 endg.: Mitteilung der Kommission an das Europäische Parlament, den Rat und den Ausschuss der Regionen: Eine allgemeine Politik zur Bekämpfung der Internetkriminalität v. 22.5.2007.

[256] KOM (2007) 267 endg., S. 9.

[257] KOM (2009) 149 endg.: Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen über den Schutz kritischer Informationsinfrastrukturen: „Schutz Europas vor Cyber-Angriffen und Störungen großen Ausmaßes: Stärkung der Abwehrbereitschaft, Sicherheit und Stabilität“.

[258] KOM (2010) 245 endg./2: Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen: Eine Digitale Agenda für Europa.

[259] KOM (2010) 245 endg., S. 3 ff.

hätten.[260] Die in Kapitel 3 vertieft behandelte Richtlinie über Angriffe auf Informationssysteme[261] bildet damit einen wichtigen Baustein im Streben nach europäischer Informationssicherheit. Sie wurde daher auch bereits in der Digitalen Agenda als siebte Schlüsselaktion bezeichnet und als Legislativmaßnahme angekündigt.[262]

Die Mitteilung zur Einrichtung eines Zentrums zur Bekämpfung der Cyberkriminalität[263] stellt gewissermaßen eine europäische Antwort auf den grenzüberschreitenden Charakter dieser Kriminalitätserscheinung dar. Dieses Europäische Zentrum zur Bekämpfung der Cyberkriminalität ist mittlerweile in Europol integriert und dient sowohl Mitgliedstaaten als auch EU-Agenturen, internationalen Partnern, dem Privatsektor, Forschungsgesellschaften und gesellschaftlichen Organisationen als Plattform zur Zusammenarbeit.

Als vorläufiger Höhepunkt der Kommissions-Mitteilungen zur Computerkriminalität ist die Cybersicherheitsstrategie[264] zu nennen. Diese basiert auf der Prämisse, dass die Vollendung eines europäischen digitalen Binnenmarkts eine jährliche Steigerung des EU-BIP um fast 500 Mrd. EUR einbringen könnte.[265] Dazu sei es jedoch notwendig, die Europäische Union zum sichersten Online-Umfeld der Welt zu machen. Dabei geht die Mitteilung davon aus, dass die Cyberkriminalität eine der am schnellsten wachsenden Kriminalitätsformen sei, sich bei geringem Risiko (Straftäter würden häufig die Anonymität der Internetdomänen nutzen) als sehr profitabel erweise und die Straftaten in der Regel grenzüberschreitend begangen würden. Daher habe auch die Strafverfolgung kollektiv, koordiniert und transnational zu erfolgen. Als konkrete Maßnahmen werden die Sicherstellung einer raschen Umsetzung von zu erlassenen Richtlinien zur Cyberkriminalität[266] sowie die Aufforderung an die Mitglied-

---

[260] Vgl. KOM (2010) 245 endg., S. 6.

[261] Siehe unten, Kap. 3 § 11.

[262] KOM (2010) 245 endg., S. 20 f.

[263] KOM (2012) 140 endg.: Mitteilung der Kommission an den Rat und das Europäische Parlament: Kriminalitätsbekämpfung im digitalen Zeitalter: Errichtung eines Europäischen Zentrums zur Bekämpfung der Cyberkriminalität.

[264] JOIN (2013) 1 final: Gemeinsame Mitteilung an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen: Cybersicherheitsstrategie der Europäischen Union – ein offener, sicherer und geschützter Cyberraum.

[265] Copenhagen Economics, The Economic Impact of a European Digital Single Market, 2010, S. 35; abrufbar unter: http://www.epc.eu/dsm/2/Study_by_Copenhagen.pdf (Stand: 07.08.2017).

[266] Als Ergebnisse sind bislang die Richtlinie 2011/93/EU zur Bekämpfung des sexuellen Missbrauchs und der sexuellen Ausbeutung von Kindern sowie der Kinderpornografie (siehe auch unten, Kap. 3 § 10) und die Richtlinie 2013/40/EU über Angriffe auf Informationssysteme (siehe auch unten, Kap. 3 § 11) umgesetzt worden.

staaten zur schnellstmöglichen Ratifizierung und Umsetzung der Cybercrime Convention genannt. Daneben sollen auf operativer Ebene die Mitgliedstaaten in die Lage versetzt werden, den Cyberkriminellen mindestens auf technologischer Augenhöhe zu begegnen, was durch Forschungs- und Entwicklungsprogramme sowie pan-europäische Kooperationsinitiativen sichergestellt werden soll. Zusätzlich zur Unterstützung der Mitgliedstaaten auf nationaler Ebene und durch Koordinierung der Institutionen und Ressourcen auf EU-Ebene enthält die Europäische Cybersicherheitsstrategie eine globale Dimension. Durch einen Dialog mit internationalen Partnern und internationalen Organisationen wie dem Europarat, der OECD, OSZE, der NATO und den Vereinten Nationen soll die friedliche, offene und transparente Nutzung der Cybertechnologien gewährleistet werden.

Die Cybersicherheitsstrategie greift damit viele Punkte auf, die gemeinhin als wichtig zur effektiven Bekämpfung der Computerkriminalität erachtet werden. Sie enthält Absichtserklärungen zu drei Hauptbereichen: technische Weiterentwicklung der europäischen und mitgliedstaatlichen Strafverfolgungsorgane, Koordination und Zentralisierung von Informationen zwischen den verschiedenen Akteuren sowie den Abbau rechtlicher Hemmnisse bei der Bekämpfung, Verfolgung, Aufklärung und Verurteilung transnationaler Computerkriminalität.

IV. Rahmenbeschlüsse

Bis zum Inkrafttreten des Vertrags von Lissabon, wodurch die Richtlinie als Harmonisierungsmaßnahme eingeführt wurde, bezeichnete der Rahmenbeschluss die einschlägige legislative Maßnahme der Europäischen Union auf dem Gebiet des Strafrechts. Hier weisen der Rahmenbeschluss zur Bekämpfung von Betrug und Fälschung im Zusammenhang mit unbaren Zahlungsmitteln[267] und der Rahmenbeschluss über Angriffe auf Informationssysteme[268] Berührungspunkte zum Computerstrafrecht auf. Eine dezidierte Darstellung und Auseinandersetzung mit diesen beiden EU-Rechtsakten findet sich im dritten Teil der Arbeit.[269]

V. Richtlinien

Als aktuell einschlägige Handlungsform auf dem Gebiet des Strafrechts der Europäischen Union ist gem. Art. 83 AEUV die Richtlinie anzuführen. Mit Bezug

---

[267] Rahmenbeschluss 2001/413/JI v. 28.5.2001 zur Bekämpfung von Betrug und Fälschung im Zusammenhang mit unbaren Zahlungsmitteln, ABl. L 149 v. 2.6.2001, S. 1.

[268] Rahmenbeschluss 2005/222/JI v. 24.2.2005 über Angriffe auf Informationssysteme, ABl. L 69 v. 16.3. 2005, S. 67 (mittlerweile durch RL 2013/40/EU ersetzt).

[269] Siehe unten, Kap. 3 § 9 und Kap. 3 § 11.

zur Computerkriminalität sind die Richtlinie zur Bekämpfung des sexuellen Missbrauchs von Kindern[270] und die Richtlinie über Angriffe auf Informationssysteme[271] zu nennen. Auch bezüglich dieser beiden Richtlinien sei an dieser Stelle auf deren ausführliche Behandlung in Teil 3 der Arbeit verwiesen.[272]

§ 3 Zusammenfassung

Auf dem europäischen Kontinent sind die Europäische Union und der Europarat die supra- bzw. internationalen Institutionen, die im materiellen Strafrecht und insbesondere auch im Computerstrafrecht Rechtsnormen schaffen können. Eine Harmonisierung des materiellen Computerstrafrechts findet durch den Europarat im Wege völkerrechtlicher Vereinbarungen statt. Die Europäische Union bedient sich seit dem Vertrag von Lissabon gemäß Art. 83 Abs. 1 AEUV der Richtlinie als Handlungsform. Keine der beiden Rechtsetzungsformen entfaltet in den jeweiligen Mitgliedstaaten eine unmittelbare Wirkung für die rechtsunterworfenen Bürger. Vielmehr verpflichten sie die Mitgliedstaaten zur Umsetzung in nationales Recht und stellen daher sog. Strafanweisungsrecht dar.

Die Europäische Union erlässt Richtlinien, die hinsichtlich ihrer Ziele verbindlich sind und den Mitgliedstaaten die Umsetzung innerhalb einer bestimmten Frist auferlegen. In der Theorie wird dadurch die Souveränität der Legislativorgane der einzelnen Mitgliedstaaten möglichst weitgehend geachtet. In der Praxis hingegen werden die Mitgliedstaaten durch die Anweisungskompetenz der Europäischen Union dazu verpflichtet, auf Basis des Art. 83 AEUV strafrechtliche Sanktionen zu verschärfen oder neu einzuführen, sodass die Freiheit der Form der Umsetzung faktisch doch erheblich eingeschränkt wird.[273] Bei Nichtumsetzung drohen den Mitgliedstaaten Vertragsverletzungsverfahren mit Strafzahlungen oder gegebenenfalls sogar die unmittelbare Wirkung der jeweiligen Richtlinie, die ansonsten der Handlungsform der Verordnung vorbehalten ist. Diese eigentlich dem Wortlaut von Art. 288 Abs. 3 AEUV widersprechende Rechtsfortbildung[274] wird einerseits auf das Effektivitätsprinzip (*effet utile*)[275]

---

[270] Richtlinie 2011/93/EU zur Bekämpfung des sexuellen Missbrauchs und der sexuellen Ausbeutung von Kindern sowie der Kinderpornografie sowie zur Ersetzung des Rahmenbeschlusses 2004/68/JI, ABl. L 335 v. 17.12.2011, S. 1.

[271] Richtlinie 2013/40/EU v. 12.8.2013 über Angriffe auf Informationssysteme und zur Ersetzung des Rahmenbeschlusses 2005/222/JI, ABl. L 218 v. 14.8.2013, S. 8.

[272] Siehe unten, Kap. 3 § 10 und Kap. 3 § 11.

[273] *Safferling*, Internationales Strafrecht, § 9 Rn. 86.

[274] Zum Begriff in diesem Zusammenhang siehe *Herrmann*, Richtlinienumsetzung, S. 40 ff.

[275] EuGH, Rs. 41/74, Slg. 1974, 1337, Rn. 12 – *van Duyn/Home Office*; Rs. 51/76, Slg.

und andererseits auf den Grundsatz von Treu und Glauben[276] gestützt. Dadurch soll verhindert werden, dass die Bürger der Mitgliedstaaten eine unterschiedliche Rechtsposition vor den Gerichten erhalten und dass die mitgliedstaatliche Säumnis Einzelnen zum Nachteil gereicht.[277]

Der Europarat, als zweiter internationaler, rechtsetzender Akteur des (Computer-)Strafrechts auf dem europäischen Kontinent, ist als internationale Organisation hingegen lediglich dazu befugt, seine Mitgliedstaaten und gegebenenfalls darüber hinaus weitere Völkerrechtssubjekte dazu aufzurufen, miteinander völkerrechtliche Vereinbarungen zu schließen, die für eine unmittelbare Wirkung auf die Individuen einen nationalen Umsetzungsakt unter Anwendung nationalen Rechts erfordern.

Die Gesamtschau der Unionsmaßnahmen auf dem Gebiet der Computerkriminalität zeigt zudem, dass einzelne Maßnahmen regelmäßig auf sehr vielfältige Aspekte des Computerstrafrechts abzielen. Dabei werden in diesem Bereich keine einheitlichen, sondern stattdessen viele unterschiedliche Begrifflichkeiten verwendet. Oftmals werden Definitionen weit gefasst und häufig situationsbezogen angepasst. Daher stellt der folgende Teil die einschlägigen Begrifflichkeiten, auch in ihrer historischen Dimension, zusammen, um anschließend einen europäischen Rechtsbegriff der Computerkriminalität zu entwickeln.

1977, 113, Rn. 20 und 24 – *Nederlandse Ondernemingen*; Rs. 148/78, Slg. 1979, 1629, Rn. 21 – *Ratti*; Rs. 8/81, Slg. 1982, 53, Rn. 23 – *Becker*; Rs. C-221/88, Slg. 1990, I-495, Rn. 22 – *Busseni*; Rs. C-188/89, Slg. 1990, I-3313, Rn. 16 – *Foster/British Gas*.

[276] EuGH, Rs. 148/78, Slg. 1979, 1629, Rn. 22 – *Ratti*; Rs. 70/83, Slg. 1984, 1075, Rn. 3 – *Kloppenburg/Finanzamt Leer*; Rs. 71/85, Slg. 1986, 3855, Rn. 14 – *Federatie Nederlandse Vakbeweging*; Rs. 80/86, Slg. 1987, 3969, Rn. 8 – *Kolpinghuis Nijmegen*; Rs. C-188/89, Slg. 1990, I-3313, Rn. 16 – *Foster/British Gas*; Rs. C-221/88, Slg. 1990, I-495, Rn. 22 – *Busseni*; Rs. C-91/92, Slg. 1994, I-3325, Rn. 23 f. – *Paola Faccini Dori*.

[277] *Ruffert*, in: Calliess/ders. (Hrsg.), Art. 288 AEUV Rn. 49.

Kapitel 2

Computerkriminalität: Ein Rechtsbegriff

Computerkriminalität wird zumeist sehr ausufernd als gegen computerbasierende Systeme gerichtete oder durch computerbasierende Systeme begangene Kriminalität definiert.[1] Dies trägt dem Umstand Rechnung, dass computerbasierende Systeme sowohl als Angriffsziele dienen, als auch als Tatwerkzeuge genutzt werden können. Daher sind auch die Themen, mit denen sich nationale und internationale Institutionen in diesem Bereich beschäftigen, breit gefächert. Es ist ein immens großes Spektrum der Kriminalität einbezogen. Bisher fand vor allem der Begriff der Computerkriminalität in offiziellen Veröffentlichungen und Normen (z.B. Art. 83 Abs. 1 UAbs. 2 AEUV) Anwendung, während der Begriff der Internetkriminalität im nationalen und europäischen Diskurs an Bedeutung gewinnt.[2] Im internationalen Diskurs hingegen hat sich der Begriff des „Cybercrime“ durchgesetzt. Eine Legaldefinition besteht bislang freilich für keinen der genannten Begriffe.

Die Bedeutung begrifflicher Klarheit darf dabei nicht unterschätzt werden. So entscheidet das Verständnis von Computerkriminalität beispielsweise darüber, welche Bereiche des mitgliedstaatlichen Strafrechts von den Kompetenzen der Europäischen Union nach Art. 83 Abs. 1 UAbs. 2 AEUV erfasst sind. Auch in der Kommentarliteratur wird bereits auf die Konturlosigkeit des Computerkriminalitätsbegriffs und die damit einhergehende drohende Unbeschränktheit der Harmonisierungsmöglichkeiten durch die Europäische Union hingewiesen.[3] Diese potenzielle Weite wird noch dadurch verstärkt, dass sich die Harmonisierungskompetenz nach Art. 83 Abs. 1 UAbs. 2 AEUV zwar auf derartige Kriminalitätsbereiche bezieht, die typischerweise einen grenzüberschreitenden Cha-

[1] Siehe beispielsweise die Cybercrime Convention (ETS Nr. 185); JOIN (2013) 1 final, S. 3; KOM (2007) 267 endg., S. 3; *Clough*, Cybercrime, S. 9 ff.; *Gercke, M.*, Understanding Cybercrime Studie, 2012, S. 11 ff.; *Sieber u. a.*, Comprehensive Study on Cybercrime, 2013, S. 11 f.; die genannten Quellen nutzen teilweise den internationalen Begriff des „Cybercrime“, was freilich an der phänomenologischen Zuordnung nichts ändert.

[2] Vor allem im allgemeinen deutschen Sprachgebrauch und in Veröffentlichungen der Europäischen Union wird oftmals von „Internetkriminalität“ gesprochen.

[3] *Vogel/Eisele*, in: Grabitz/Hilf/Nettesheim (Hrsg.), 57. EL Aug. 2015, Art. 83 AEUV Rn. 62.

rakter aufweisen und Felder besonders schwerer Kriminalität betreffen – im Einzelfall muss es sich jedoch dem Wortlaut nach nicht tatsächlich um einen grenzüberschreitenden Sachverhalt handeln. Eine Zugehörigkeit zu einem der aufgezählten Kriminalitätsbereiche genügt.[4]

Obwohl sich diese Problematik nicht auf die Computerkriminalität beschränkt, sondern sich auf sämtliche in Art. 83 Abs. 1 UAbs. 2 AEUV genannten Bereiche erstreckt, ist die Computerkriminalität durch die Anknüpfung an einen Alltagsgegenstand auf besondere Weise von dieser sog. umfassenden Harmonisierung betroffen. Anders als etwa bei Kriminalitätsbereichen wie Korruption oder Terrorismus, ergibt sich die sozialschädliche Dimension der Computerkriminalität nämlich erst aus einer Kombination mit dem Begriff der „Kriminalität", da Computer zunächst einmal strafrechtlich neutral sind.

An der vom Bundesverfassungsgericht erhobenen Forderung, die Kompetenzen der Europäischen Union zur Strafrechtsharmonisierung restriktiv auszulegen,[5] lässt sich bereits das Spannungsfeld zwischen deutschem Verfassungsverständnis, insbesondere nach dem Lissabon-Urteil des Bundesverfassungsgerichts, und einer fortscheitenden Europäisierung, die auch das Strafrecht, das gemeinhin als eine der letzten nationalstaatlichen Bastionen verstanden wird, erkennen. Allerdings ist auch zu beachten, dass es der einhelligen Meinung entspricht, nur gemeinsam im europäischen oder besser noch weltweiten Verbund gegen Internet- und Computerkriminalität effektiv vorgehen zu können, da vor allem in diesem Kriminalitätsbereich weder Ländergrenzen noch kontinentale Beschränkungen für die Täter eine Rolle spielen. Eine Re-Nationalisierung kommt daher grundsätzlich nicht in Betracht. Es stellt sich daher die Frage nach einer (unions-)rechtskonformen und gleichzeitig an den Spezifika des Kriminalitätsphänomens orientierten Definition und Begrenzung des Computerkriminalitätsbegriffs.

Auch in der vorliegenden Arbeit wurde bisher nicht ausschließlich der Begriff der Computerkriminalität nach Art. 83 Abs. 1 UAbs. 2 AEUV verwendet, sondern darüber hinaus auch von „Cyberkriminalität", „Internetkriminalität" und „Hightechkriminalität" gesprochen. Dieser vorherrschende, oft durchaus zufällige Gebrauch jener Begrifflichkeiten verkennt jedoch die rechtliche Relevanz einer klaren Definition für das Unionsrecht und das Kompetenzverhältnis zwischen Europäischer Union und den Mitgliedstaaten. Daher werden die folgenden Ausführungen insbesondere zwischen einer bestmöglichen Beschreibung und Bezeichnung eines Kriminalitätsbereichs und einem hinreichend bestimmten Harmonisierungsobjekt differenzieren. Der vor allem in der Literatur

---

[4] Vgl. insoweit insb. unten, Kap. 2 § 7 B. III.

[5] BVerfGE 123, 267 (413).

geäußerten Auffassung, eine genaue Definition von Computer- und Internetkriminalität sei nicht nur sehr schwierig, sondern auch gar nicht notwendig, da es sich schließlich bei diesen nicht um Rechtsbegriffe handele,[6] ist insoweit entschieden entgegenzutreten. Durch die Aufnahme als harmonisierungsfähigen Kriminalitätsbereich in den AEUV hat zumindest der Begriff der Computerkriminalität eine rechtliche Dimension erhalten, die deutlich über die Beschreibung eines Phänomens hinausgeht. Das Verständnis dieses Terminus hat sowohl für die EU als auch für ihre Mitgliedstaaten sowie schlussendlich auch für die einzelnen EU-Bürger Konsequenzen. Dennoch ist der Begriff der Computerkriminalität weder im Primär- noch im Sekundärrecht der EU legaldefiniert. Stattdessen greifen u. a. die Organe der Europäischen Union sowie ein Großteil der Literatur regelmäßig auf die bereits angesprochenen extensiven Begrifflichkeiten der Cybercrime Convention zurück.[7]

Im Folgenden wird zunächst der Status quo dargestellt. Ausgehend von Art. 83 Abs. 1 UAbs. 2 AEUV, den dazugehörigen Gesetzgebungsmaterialien und Kommentierungen wird der Begriff der Computerkriminalität ausgelegt und in das bestehende System aus Strafrecht, Verfassungsrecht und Europarecht eingeordnet. Dabei wird Art. 83 AEUV mit seinen Gesetzgebungsmaterialien und den Kommentierungen einen Einstieg bieten. Zusätzlich wird allerdings auch eine Abgrenzung zu verwandten Begriffen wie Internetkriminalität, IuK-Kriminalität und Cyberkriminalität vorgenommen.

Den Abschluss dieses zweiten Teils bildet sodann die Erarbeitung eines neuen, schärfer umrissenen Begriffs der Computerkriminalität, der die Kritik des Bundesverfassungsgericht in dessen „Lissabon-Urteil“ aufnimmt und zugleich das Unionsrecht und seine Auslegungsgrundsätze respektiert.

§ 4 Begriffsbestimmung und Abgrenzung zu verwandten Begriffen

Bei der Definition der Computerkriminalität nach Art. 83 Abs. 1 UAbs. 2 AEUV werden zusätzlich zur deutschen Praxis und Forschung vor allem die englischen Begriffe sowie Definitionsansätze aus anderen Rechtskreisen herangezogen, um der Internationalität der Problematik gerecht werden zu können. Insbeson-

---

[6] Exemplarisch: *Gercke, M.*, Understanding Cybercrime Studie, 2012, S. 11 f.; abrufbar unter: http://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf (Stand: 07.08.2017); für den internationalen Kontext vgl. *Appazov*, Cybersecurity, S. 22 f.; ebenfalls die Relevanz einer Definition verkennend *Krischker*, Das Internetstrafrecht vor neuen Herausforderungen, S. 21.

[7] *Fahey*, EJRR 2014, 46 (47).

dere im europäischen Diskurs spielen die unterschiedlichen Sprachfassungen nicht lediglich für die Länder mit der entsprechenden Landessprache, sondern für den gesamteuropäischen Auslegungsprozess des Begriffs eine Rolle.

Während begriffliche Unschärfen im akademischen und mit Abstrichen sogar im exekutiven Kontext noch verzeihlich sein mögen, ist eine annähernde Begriffseindeutigkeit, oder zumindest deren Herstellbarkeit im Wege der Auslegung, aus legislatorischer Perspektive zwingend erforderlich, um die Rechtsunterworfenen nicht der Willkür rechtsetzender Organe auszusetzen. Dieser Grundsatz, ursprünglich zum Schutz der Bürger eines Rechtsstaats aufgestellt, hat auch im europäischen Primärrecht zumindest in Teilen Anwendung zu finden, da die Mitgliedstaaten durch dieses Primärrecht faktisch selbst zu Rechtsunterworfenen gegenüber einem Normgeber geworden sind. Es stellt sich daher erstens die Frage nach einer bestehenden Definition des Begriffs der Computerkriminalität,[8] zweitens, ob darin ein geeigneter Begriff für eine Harmonisierungsfreigabe im Primärrecht zu sehen ist,[9] und schließlich drittens, ob gegebenenfalls bestehende begriffliche Schwächen im Wege einer Auslegung bzw. Einschränkung oder Begrenzung behoben werden können.[10]

Ungefähr seit einem Jahrzehnt werden auch die Begriffe Cyberwar und Cyberterrorismus mit Cyber- bzw. Computerkriminalität in Verbindung gebracht. Eine Bearbeitung dieser Thematiken oder auch nur eine Abgrenzung zwischen Cyberwar und Cyberterrorismus[11] bieten freilich jeweils ausreichend viele Fragestellungen – u. a. mit einem starken völkerrechtlichen Fokus – für selbstständige wissenschaftliche Arbeiten, sodass hier lediglich auf zwei Aspekte verwiesen sein soll. Einerseits konzentriert sich diese Arbeit auf die Kriminalitätsbekämpfung und klammert damit Konstruktionen aus, in denen Staaten oder staatsähnliche Akteure Computer(systeme) als Mittel in kriegerischen Auseinandersetzungen verwenden.[12] Andererseits fallen die Mittel des Cyberterrorismus – solange sie nicht anhand völkerrechtlicher Zuordnungskriterien dem Kriegsrecht unterliegen –[13] in den Bereich des zivilen Sicherheits- und Straf-

[8] Siehe unten, Kap. 2 § 4 A.

[9] Siehe unten, Kap. 2 § 6 C.

[10] Siehe unten, Kap. 2 § 7.

[11] Eine Definition zur Cyberkriminalität, auch unter Berücksichtigung der meisten Cyberterrorismus-Attacken, bietet *Clough*, Cybercrime, S. 12 ff.

[12] Für eine aktuelle Auseinandersetzung mit dem Phänomen vgl. *Greathouse*, in: Kremer/Müller (Hrsg.), Cyberspace, S. 21 (23 ff.) m. w. N. und insb. hinsichtlich des anwendbaren Rechts bei kriegerischen Auseinandersetzungen im Cyberraum siehe *Schmitt*, Talinn Manual on the International Law applicable to Cyber-warfare, 2013, S. 75 ff.; siehe auch unten, Kap. 4 § 14 B. III. für einen kurzen Überblick zu den bekannten Cyberwar-Attacken „Estland“, „Georgien“ und „Stuxnet“.

[13] Besonders relevant geworden ist diese Frage im Rahmen der Attacken des aus Syrien

rechts, sodass sie ohnehin vom Computerkriminalitätsbegriff dieser Arbeit umfasst sind.

A. Forschungsstand zum Computerkriminalitätsbegriff

Wohl keiner der übrigen Kriminalitätsbereiche des Art. 83 Abs. 1 UAbs. 2 AEUV ist ähnlich weit gefasst wie derjenige der Computerkriminalität. Das liegt maßgeblich an der Tatsache, dass es sich um einen untypischen Kriminalitätsbereich handelt. Zur Beschreibung wird nicht auf einen Sammelbegriff für miteinander verwandte (z. B. Korruption) oder in sachlichem Zusammenhang stehende (z. B. Terrorismus) Straftaten zurückgegriffen, sondern ein Tatmittel oder Tatobjekt herangezogen. Die Begriffsweite spiegelt sich auch in den Ausführungen zahlreicher juristischer Abhandlungen zu diesem Kriminalitätsbereich wider: Zumeist ist ihnen eine Definition des Untersuchungsbereichs vorangestellt, in der die Verfasser jedoch regelmäßig zu dem Schluss kommen, dass aufgrund der Konturlosigkeit des Begriffs nur eine näherungsweise Bestimmung erfolgen könne.[14] Einen einheitlich anerkannten Begriff der Computerkriminalität gibt es demnach, trotz zahlreicher wissenschaftlicher Anstrengungen, bislang nicht.[15]

Die Definition des Begriffs der Computerkriminalität hat seit seinem erstmaligen Auftreten in den 1970er-Jahren eine Entwicklung durchgemacht, die sich einerseits mit dem Fortschritt der technischen Möglichkeiten im Computertechnologiebereich erklärt, andererseits aber auch durch Betrachtung der mit der jeweiligen Begriffsbestimmung verfolgten Ziele verstanden werden kann. In der deutschen Forschung gehen die Anfänge der Begriffsarbeit auf *von zur Mühlen* zurück. Er hat unter dem Begriff der Computerkriminalität zunächst all jenes deliktische Handeln verstanden, bei welchem der Computer entweder Werkzeug oder Ziel der Tat ist.[16] Ein Jahr später schränkte er seine Definition

---

und Irak heraus agierenden Islamischen Staats auf Paris im November 2015. Rechtliche Relevanz gewann die Abgrenzung zwischen kriegerischen Handlungen und terroristischen Angriffen durch die Zuordnung der Unterstützungsanforderung der französischen Regierung gegenüber den EU-Mitgliedstaaten, da sich diese entweder nach Art. 42 Abs. 7 EUV (Kriegsfall) oder Art. 222 AEUV (Terrorangriff) richten könnte. Frankreich entschied sich, wohl im Einklang mit dem Völkerrecht (im Detail untersuchen *Peterke/Noortman*, AdV 53 (2015), 1 ff. die Völkerrechtssubjektivität bzw. völkerrechtliche Einordnung transnational agierender Terrororganisationen), für das Kriegsrecht.

[14] So etwa: *Hirsnik*, Strafbarkeit eines Angriffs auf das Computersystem, S. 2.

[15] So u. a. *Appazov*, Cybersecurity, S. 23; *Dorra*, Legislativkompetenzen, S. 209; *Fahey*, EJRR 2014, 46 (50); *Tropina*, in: dies./Callanan (Hrsg.), Self- and Co-regulation in Cybercrime, Cybersecurity and National Security, S. 5; *Watney*, JITST 2012, 61 (62).

[16] *von zur Mühlen*, Computer-Kriminalität, S. 17.

dahin gehend ein, dass „die Tat nur mit Hilfe des Computers möglich oder stark erleichtert, oder aber ihre Entdeckung durch den Computer verhindert wurde“.[17] *Lampe* fasst dasjenige kriminelle Verhalten unter den Begriff der Computerkriminalität, dessen Mittel oder Zweck das pflichtwidrige Einwirken auf die elektronische Datenverarbeitung darstellt, hält aber davon ausgehend eine Typisierung der kriminellen Verhaltensweisen nach strafrechtlichen Kriterien für zwingend geboten.[18] Ebenfalls in den 1970er-Jahren entwickelte sich in den Vereinigten Staaten von Amerika ein Verständnis von Computerkriminalität, das neben der Deliktsausführung auch aus Tataufklärungsperspektive an eine Definition heranging: „any illegal act for which knowledge of computer technology is essential for a successful prosecution“ [deutsch: „jede illegale Aktivität, zu deren erfolgreicher Verfolgung Kenntnisse in der Computertechnologie erforderlich sind“][19]. Der Europarat hingegen versucht sich in seiner Empfehlung 1989 nicht an einer eigentlichen Definition, sondern wählt stattdessen einen eher pragmatischen Ansatz: Danach sind diejenigen Delikte Computerkriminalität, die in die Empfehlung aufgenommen wurden.[20]

Sobald anerkannt wurde, dass die „Computerkriminalität“ tatsächlich wissenschaftliche und praktische Relevanz hat,[21] begannen Teile der Strafrechtswissenschaft, Deliktsgruppen zu bilden, die von einer etwaigen Definition umfasst werden sollten. Dieser Versuch resultierte aus Zweifeln, ob eine einheitliche Definition auf nicht phänomenologischem Wege erreichbar wäre.[22]

Herausgebildet hat sich daher letztlich ein kleinster gemeinsamer Nenner – der allerdings versucht, sämtliches strafwürdiges Verhalten, das einen Computer involviert oder tangiert, zu erfassen und daher eher als „größte gemeinsame Summe“ bezeichnet werden sollte. Nach gängigem weiten Verständnis sind dabei in der Regel vier Gruppen von Straftaten einbezogen: erstens Straftaten, bei denen Computersysteme und -daten als Angriffsobjekte fungieren, zweitens Straftaten, bei denen Computer als Angriffsmittel bzw. Tatwerkzeuge eingesetzt werden, drittens inhaltsbezogene Straftaten, bei denen Computer zur Verbreitung illegaler Inhalte eingesetzt werden, und schließlich viertens Delikte,

---

[17] Vgl. *Sieber*, DSWR 1974, 245 (246).

[18] *Lampe*, GA 1975, 1.

[19] *Parker*, SRI International, Computer crime: criminal justice resource manual – U.S. Dept. of Justice, 1979, S. 3; die aktualisierte Fassung des Manuals von 1989 (dort findet sich die zitierte Definition auf S. 2) ist abrufbar unter: https://www.ncjrs.gov/pdffiles1/Digitization/118214NCJRS.pdf (Stand: 07.08.2017).

[20] Council of Europe, Recommendation No. R (89) 9 on computer-related Crime, 1990, S. 14.

[21] Das anzweifelnd: *Betzl*, DSWR 1972, 475 ff.; dagegen: *Sieben/von zur Mühlen*, DSWR 1972, 397 ff.

[22] Exemplarisch: *Gercke, M./Brunst*, Internetstrafrecht, Kap. 3 Rn. 73.

die sich mittels der Verwendung von Computern gegen das Urheberrecht wenden.[23] Dieses Begriffsverständnis findet sich nicht nur regelmäßig in der Kommentarliteratur zu Art. 83 Abs. 1 UAbs. 2 AEUV. Auch die Europäische Kommission arbeitet mit dieser Definition.[24] Maßgeblich für die Verbreitung dieser Begriffsbestimmung dürfte vor allem die Cybercrime Convention des Europarats gewesen sein, die selbst jene viergliedrige Schutzrichtung aufweist. Dass diese Schutzweite nicht mit dem gegebenenfalls enger zu verstehenden Begriff der Cyberkriminalität zusammenpasst,[25] hat sich bisher allerdings lediglich in der deutschen Europarats-Übersetzung der Cybercrime Convention niedergeschlagen, die mit dem Titel „Übereinkommen zur Computerkriminalität" operiert, obwohl eine möglichweise stärker am englischen Originaltext („Cybercrime") orientierte Übersetzung mit „Übereinkommen zur Datennetzkriminalität", wie sie auch das BMJ nutzt,[26] durchaus zur Verfügung stünde.

Selbst in aktuellsten Arbeiten findet sich weitgehend entweder die Ansicht, dass der Computer bzw. die EDV-Anlage als Tatmittel oder Tatobjekt fungiert,[27] oder dass anstelle einer echten Definition vielmehr ein „Straftaten-Katalog" zu bilden sei („basket of acts"), sodass der Forschungsfokus besser auf die jeweils zu bestrafende Handlung gelegt werden könne.[28] Ähnlich argumentiert *Gercke*, der sich zwar mit der Begriffsthematik auseinandersetzt und unter Bezug auf Ausarbeitungen der Vereinten Nationen[29] zwischen „computer crime" und „computer-related crime" unterscheidet, letztlich aber ebenfalls, wie *Sieber u. a.* in der UNODC-Studie[30], zu dem Schluss kommt, dass eine exakte Definition einerseits schwierig zu finden und andererseits auch gar nicht nötig sei, solange man die Begriffe nicht als sog. Rechtsbegriffe verwende.[31]

[23] *Böse*, in: Schwarze (Hrsg.), Art. 83 AEUV Rn. 13; *Vogel/Eisele*, in: Grabitz/Hilf/Nettesheim (Hrsg.), 57. EL Aug. 2015, Art. 83 AEUV Rn. 62; *Gercke, M./Brunst*, Internetstrafrecht, Kap. 3 Rn. 74.

[24] KOM (2007) 267 endg., S. 1.

[25] Siehe unten, Kap. 2 § 4 B. II.

[26] Siehe dazu *Spannbrucker*, Computerstrafrecht, S. 9.

[27] *Bär*, in: Wabnitz/ders. (Hrsg.), Handbuch des Wirtschafts- und Steuerstrafrechts, Kap. 12 Rn. 9; *Jones*, Mobile internetfähige Geräte im Strafrecht, S. 73.

[28] Explizit bzgl. Cybercrime, aber durchaus generalisierbar: *Sieber u. a.*, Comprehensive Study on Cybercrime, 2013, S. 12.

[29] UNODC, Crimes related to computer networks – Background paper for the workshop on crimes related to the computer network, 10th UN Congress on the Prevention of Crime and the Treatment of Offenders, 2000, A/CONF.187/10, S. 5; abrufbar unter: https://www.unodc.org/documents/congress//Previous_Congresses/10th_Congress_2000/017_ACONF.187.10_Crimes_Related_to_Computer_Networks.pdf (Stand: 07.08.2017).

[30] *Sieber u. a.*, Comprehensive Study on Cybercrime, 2013, S. 11 f.

[31] *Gercke, M.*, Understanding Cybercrime Studie, S. 11 f.

Vereinzelt haben Autoren, die sich mit einer rein phänomenologischen Betrachtungsweise nicht zufriedengeben, versucht, den Bereich der Computerkriminalität klarer zu umreißen. *Schuh* etwa plädiert für eine Eingrenzung des Begriffs dahin gehend, dass der Computer bei der Begehung der Straftat entweder als zwingend erforderliches Tatmittel fungiert oder auf Seiten des Tatobjekts der deliktischen Handlung eine wesentliche Rolle spielt.[32] Auch *Hilgendorf* merkte richtigerweise an, dass sich nahezu sämtliche Straftaten mithilfe des Internets begehen ließen, und regt daher den Begriff der Datennetzkriminalität für einen engeren Straftatenkatalog an.[33]

Piazena will insbesondere eine klare Abgrenzung zwischen der Computerkriminalität und der Internetkriminalität erzielen. Unter Computerkriminalität i. e. S. versteht er diejenigen Deliktstatbestände, die das Rechtsgut der Integrität von Daten und Datenverarbeitungsanlagen schützen und im Wesentlichen durch das 2. WiKG[34] in das Strafgesetzbuch aufgenommen und teilweise durch das 41. StrÄndG[35] erweitert worden sind. Diese Computerkriminalität i. e. S. sei nicht auf einen Datenaustausch angewiesen. Dadurch sei eine klare Abgrenzung zur Internetkriminalität in der Regel unproblematisch. Computerkriminalität i. w. S. sieht *Piazena* als Oberbegriff für die Computerkriminalität i. e. S. und die Internetkriminalität an. Hierunter fielen sowohl die klassischen Computerdelikte als auch alle mithilfe des Internets begangenen Straftaten.[36]

Ausgehend von einem extensiven Begriffsverständnis zählt *Hecker* zur Computerkriminalität all jene „Kriminalitätsphänomene, die unmittelbar oder mittelbar im Zusammenhang mit der elektronischen Datenverarbeitung stehen und unter Einbeziehung einer EDV-Anlage (als Tatmittel und/oder Tatobjekt) begangen werden".[37] Im zweiten Schritt grenzt er diese weite Definition jedoch durch eine enumerative Aufzählung der möglichen Erscheinungsformen der Computerkriminalität – Computerspionage, Computersabotage, Computermanipulationen und die unberechtigte Nutzung von Computern und Programmen – auf einen dann eher engen Computerkriminalitätsbegriff ein.[38]

---

[32] *Schuh*, Computerstrafrecht im Rechtsvergleich, S. 28.

[33] *Hilgendorf*, ZStW 113 (2001), 650 (653); ihm zustimmend später *Gercke, B.*, GA 2012, 474 (475).

[34] Zweites Gesetz zur Bekämpfung der Wirtschaftskriminalität v. 15.5.1986, in Kraft getreten zum 1.8.1986, BGBl. I 1986, S. 721.

[35] 41. Strafrechtänderungsgesetz v. 7.8.2007, in Kraft getreten zum 11.8.2007, BGBl. I 2007, S. 1786.

[36] *Piazena*, Kommunikationsmöglichkeiten des Internets, S. 112 ff.

[37] *Hecker*, Europäisches Strafrecht, Kap. 11 Rn. 86.

[38] *Hecker*, Europäisches Strafrecht, Kap. 11 Rn. 86; so sah es auch schon *Abu-Zeitoun*, Computerdelikte, S. 3.

In eine ähnliche Richtung geht auch bereits der Rahmenbeschluss über Angriffe auf Informationssysteme,[39] der eine Strafbarkeitsangleichung für den rechtswidrigen Zugang zu Informationssystemen (Art. 2), den rechtswidrigen Systemeingriff (Art. 3) und den rechtswidrigen Eingriff in Daten (Art. 4) fordert und sich damit von der schier endlos weiten Definition der Cybercrime Convention des Europarates absetzt. Die den Rahmenbeschluss ersetzende Richtlinie über Angriffe auf Informationssysteme[40] erweitert die Materie zwar um das rechtswidrige Abfangen von Daten, bietet aber durch Aufzählung relevanter Tathandlungen ebenfalls eine Begrenzung. Mit diesen Beschränkungen in Rahmenbeschluss und Richtlinie hat die EU freilich keine Aussage darüber getroffen, ob damit der Bereich der Computerkriminalität umfassend abgedeckt oder lediglich ein Teilaspekt in diesen Rechtsakten aufgegriffen worden ist.

Wesentlich einfacher macht es sich hingegen etwa *Kochheim*, wenn er den Begriff der Computerkriminalität ausschließlich semantisch untersucht und daher zu dem Schluss kommt, dass Computer für sich genommen lediglich unvernetzte informatisch arbeitende Datenverarbeitungssysteme sind.[41] Ihm folgend wäre die Computerkriminalität letztlich auf ganz eng umgrenzte Fälle krimineller Handlungen an einem Computer zu beschränken, sodass Vernetzungskomponenten in diesem Zusammenhang – anders ggf. in den Bereichen der Internet- oder Cyberkriminalität – keinerlei Bedeutung zukäme.

Aus dem oben Gesagten folgt, dass sich der Großteil sowohl der rechtswissenschaftlichen Forschung als auch der europäischen Institutionen mit einer phänomenologisch-typisierenden Betrachtung des Kriminalitätsbereichs zufriedengibt. Über einen gewissen Kernbereich der Computerkriminalität hinaus, der die klassischen sog. computerspezifischen bzw. computerbezogenen Delikte, die sich in der Regel gegen die Vertraulichkeit, Integrität und Verfügbarkeit von Computersystemen richten,[42] umfasst, werden sämtliche Straftaten einbezogen, die mithilfe eines Computers verwirklicht werden können. Dadurch werden auch klassische Delikte, inhaltsbezogene Delikte und Urheberrechtsstraftaten zu Erscheinungsformen der Computerkriminalität.[43] Obwohl sich die europäische Politik bislang zwar in der praktischen Umsetzung, wie noch zu zeigen sein wird, eher an einem engen Computerkriminalitätsbegriff

---

[39] ABl. 2005 L 69 v. 16.3.2005, S. 67.
[40] ABl. L 218 v. 14.8.2013, S. 8.
[41] *Kochheim*, Cybercrime und Strafrecht, Kap. 1 Rn. 45.
[42] *Sieber*, in: ders./Satzger/von Heintschel-Heinegg, Europäisches Strafrecht, § 24 Rn. 2.
[43] Bei *Walter*, JZ 2015, 685 (687), ist allerdings durchaus eine Sensibilität für die Problematik zu erkennen, wenn er inhaltsbezogene und gegen das Urheberrecht gerichtete Computerstraftaten exkludiert und infolgedessen von *cyber incidents* spricht, um die Besonderheit des modernen Kriminalitätsbereichs herauszustellen.

orientiert, indem sie ihre Harmonisierungsanstrengungen auf computerspezifische bzw. computerbezogene Delikte beschränkt, ist eine zukünftige extensive Auslegung aufgrund der Definitionen in Mitteilungen und Programmen ebenfalls wahrscheinlich.

B. Abgrenzung zu weiteren Begriffen

Weil der Begriff der Computerkriminalität historisch als Ausgangspunkt (engl.: *computer crime* und *computer-related crime*) der Begriffsdebatte gesehen werden kann und weil er auch aktuell durch seine Verankerung in Art. 83 Abs. 1 UAbs. 2 AEUV ausschlaggebend bleibt, ist eine Abgrenzung zu verwandten, in Wissenschaft und Praxis oft verwendeten Begriffen notwendig, bevor eine positive Definition versucht wird.

I. Internetkriminalität

Vielleicht spricht die Tatsache, dass *Internet* noch moderner klingt als *Computer*, dafür, „Internetkriminalität“ zu untersuchen – und dabei regelmäßig und nahezu argumentationslos die Vorarbeiten zum Computerkriminalitätsbegriff zu übernehmen.[44] Obwohl der Begriff der Internetkriminalität häufig als Synonym[45] oder als Weiterentwicklung[46] der Computerkriminalität verwendet wird, geht schon aus dem Wortlaut hervor, dass es sich um einen Unterfall handeln muss.[47] Simpel formuliert handelt es sich bei computerstrafrechtlichen Delikten zugleich um Fälle der Internetkriminalität, wenn diese unter Ausnutzung des Internets begangen werden.[48] In diesem Sinne werden unter Internetkriminalität alle Delikte subsumiert, die mittels elektronischer Kommunikationsnetze und Informationssysteme begangen werden oder sich gegen solche Netze und Systeme richten.[49]

---

[44] *Meier*, MschrKrim 2012, 184 (187 f.), weist wenigstens darauf hin, dass die Begrifflichkeiten im Wandel sind und auch das BKA für seine Statistiken auf unterschiedliche Begriffe zurückgreift.

[45] *Marberth-Kubicki*, Computer- und Internetstrafrecht, S. 50, etwa geht davon aus, dass eine Unterscheidung zwischen den Begriffen der Computer- und Internetkriminalität (fast) überflüssig geworden ist, da die Schnittmengen sehr umfangreich sind.

[46] KOM (2007) 267 endg., S. 2.

[47] So auch *Eisele*, Computer- und Medienstrafrecht, § 1 Rn. 1; *Hilgendorf/Valerius*, Computer- und Internetstrafrecht, § 1 Rn. 7; *Paramonova*, Cyberspace, S. 34; *Schuh*, Computerstrafrecht im Rechtsvergleich, S. 29; *Sieber*, in: ders./Satzger/von Heintschel-Heinegg, Europäisches Strafrecht, § 24 Rn. 1; *Vetter*, Internetkriminalität, S. 13.

[48] *Sieber*, in: ders./Satzger/von Heintschel-Heinegg, Europäisches Strafrecht, § 24 Rn. 1.

[49] *Schuh*, Computerstrafrecht im Rechtsvergleich, S. 29; auch schon von diesem weiten

Vor allem *Vetter*[50] und *Paramonova*[51] stellen sich die Frage, ob es bei der Internetkriminalität nicht um eine gänzlich neue Kriminalitätsform gehen könnte, und beziehen sich dabei auf *Vassilaki*[52], die damit argumentiert, dass es sich bei den Tatmitteln bzw. Tatobjekten schließlich nicht mehr um automatische Datenverarbeitungsanlagen, sondern vielmehr um Datennetze handele und somit ein neues Phänomen entstanden sei.

Auch wenn der Begriff der Internetkriminalität also ein Minus zur Computerkriminalität darstellt, sind seine Konturen nicht ausreichend klar umrissen. Denn die Tatsache, dass heutzutage nahezu sämtliche Datenverarbeitungsanlagen zumindest zeitweilig mit dem Internet verbunden sind, erschwert eine Unterscheidung zwischen Computer- und Internetdelikten. Ein begrenzender Impuls geht daher lediglich von *Piazenas* o. g. Ansatz einer Gliederung in Computerkriminalität i. w. S. als Oberbegriff für Computerkriminalität i. e. S. einerseits und Internetkriminalität andererseits aus.[53] Letztlich findet regelmäßig also lediglich ein Austausch der Begriffe *Computer* und *Internet* statt, sodass sich die Weite des Computerkriminalitätsbegriffs fortsetzt.

II. Cyberkriminalität

Ursprünglich geht der Begriff Cyberkriminalität auf den Wortteil „cyber" für lenken/steuern zurück,[54] wird jedoch mittlerweile vor allem als Vorsilbe für zusammengesetzte Cyber-Begriffe (z. B. Cyberspace) verwendet, sodass auch hier auf die Internet- und Netzwerkdimension abgestellt wird.[55] Vor allem im englischsprachigen Raum und im internationalen Kontext (vgl. etwa die Cybercrime Convention), aber auch in der deutschen rechtswissenschaftlichen Literatur[56] sowie in Verlautbarungen der Europäischen Union und schließlich in Institutionsbezeichnungen (vgl. European Cybercrime Center als Abteilung von

---

Begriff ausgehend *Hilgendorf/Valerius*, Computer- und Internetstrafrecht, § 1 Rn. 7; *Rüther*, in: Cimichella u. a. (Hrsg.), Technologie und Kriminalität, S. 85 (99).

[50] *Vetter*, Internetkriminalität, S. 12.

[51] *Paramonova*, Cyberspace, S. 33 f.

[52] *Vassilaki*, CR 1997, 297 (298), die allerdings den Begriff der Multimedialen Kriminalität für angebracht hält.

[53] Bemerkenswert differenziert beschäftigt sich auch bereits *Eser*, in: Leipold (Hrsg.), Rechtsfragen des Internet und der Informationsgesellschaft, S. 303 (310 ff.) mit verschiedenen Erscheinungsformen, die unter den Internetkriminalitätsbegriff subsumiert werden könnten.

[54] *Wiener*, Kybernetik.

[55] *Sieber*, in: ders./Satzger/von Heintschel-Heinegg, Europäisches Strafrecht, § 24 Rn. 1.; *Spannbrucker*, Computerstrafrecht, S. 9.

[56] *Kochheim*, Cybercrime und Strafrecht, Kap. 1 Rn. 44, kritisiert jedoch die englisch-deutsche Kombination und regt eine Verwendung des Begriffs „Cybercrime" an.

EUROPOL) wird der Begriff rege genutzt. Während häufig lediglich eine synonyme Verwendung zu Internet- bzw. Computerkriminalität anzutreffen ist,[57] findet andernorts durchaus eine Auseinandersetzung mit dem Begriff statt. Insbesondere *Paramonova*[58] und *Brodowski/Freiling*[59] erkennen in der Cyberkriminalität einen Oberbegriff. Nach *Paramonova* schließt er auch weitere Technologien, wie etwa Smartphones ein.[60] Letztere subsumieren darunter „alle Verhaltensweisen, die verfassungsrechtlich legitim unter Strafe gestellt sind oder werden könnten, und die entweder als Angriffsobjekt oder als Begehungsmittel informationstechnische Systeme einsetzen".[61] Auch der sog. Stanford-Draft arbeitet mit einer ähnlich weiten Definition und bezeichnet „Cybercrime" als illegales Verhalten unter Einbeziehung eines Computersystems.[62]

Spezifischere Definitionen stellen in der Regel auf die Notwendigkeit der Nutzung eines Netzwerks als Angriffsmittel oder -ziel ab.[63] In die gleiche Richtung argumentiert *Gercke*, der den Begriff der Cyberkriminalität als einen einschränkenden gegenüber der Computerkriminalität betrachtet, da ersterer die Einbeziehung von Computernetzwerken voraussetze.[64] *Schjolberg/Hubbard* schränken dergestalt ein, dass unter Cyberkriminalität lediglich Angriffe auf die Infrastruktur von Computersystemen und auf Netzwerke des Internets zu verstehen seien, während inhalts- und urheberrechtsbezogene Straftaten nicht unter den Terminus Cyberkriminalität zu subsumieren seien, da sie bereits in der analogen Welt Straftaten darstellten.[65]

---

[57] Beispielhaft: KOM (2007) 267 endg., S. 2; *Yi*, Die Verhältnismäßigkeit im Cyberstrafrecht, S. 54; diese Gleichstellung ist auch im internationalen Kontext anzutreffen, beispielhaft dafür: *Gordon/Ford*, Journal in Computer Virology 2006, Vol. 2, Nr. 1, 13 (14).

[58] *Paramonova*, Cyberspace, S. 34.

[59] *Brodowski/Freiling*, Cyberkriminalität, S. 30.

[60] Vgl. auch *MacQuade*, Encyclopedia_of_Cybercrime, S. 43: „Cybercrime is a broad term covering all the ways in which computers and other types of portable electronic devices such as cell phones and PDAs capable of connecting to the Internet are used to break laws and cause harm."

[61] *Brodowski/Freiling*, Cyberkriminalität, S. 30.

[62] Der sog. Stanford-Draft ist eine erste transdisziplinäre Modell-Konvention zur Bekämpfung von Computerkriminalität und stellt das Ergebnis einer internationalen Konferenz im Jahre 1999 dar; siehe *Sofaer/Goodman/Cuéllar*, The Transnational Dimension of Cybercrime and Terrorism, S. 250.

[63] Beispielhaft: *Hale*, Crime & Justice International, 18 (2002), 24.

[64] *Gercke, M.*, Understanding Cybercrime Studie, 2012, S. 11.

[65] *Schjølberg/Hubbard*, „Harmonizing National Legal Approaches on Cybercrime", ITU, Document CYB/04, 2005, S. 5.; siehe auch *Schjølberg*, History of Global Harmonization on Cybercrime Legislation, S. 9; abrufbar unter: http://www.cybercrimelaw.net/documents/cybercrime_history.pdf (Stand: 07.08.2017); wohl auch in diese Richtung zu verstehen ist *Sandywell*, in: Jewkes/Yar (Hrsg.), Handbook of Internet Crime, S. 38 (46).

Noch einen Schritt weiter geht *Koops*, der von „high end" sowie *sui generis* „cyber crimes" spricht und damit Straftaten meint, die ausschließlich in Verbindung mit dem Internet realisierbar sind. Bei jenen sei dann auch gar nicht mehr die Frage entscheidend, ob das Internet Angriffswerkzeug oder -objekt sei, sondern inwiefern sich Kriminalität grundsätzlich durch das Internet wandele und dadurch neue Formen von Angreifer-Opfer-Beziehungen hervorrufe.[66]

Wie gezeigt, erstreckt sich das Spektrum der Begriffsbestimmungen zur Cyberkriminalität von derjenigen eines Oberbegriffs für sämtliche Formen der Kriminalität, die sich technischer Hilfsmittel bedient, über eine begriffliche Gleichstellung mit der Computerkriminalität auf der einen oder der Internetkriminalität auf der anderen Seite bis hin zu einer Kriminalitätsform *sui generis*, die ausschließlich solche Straftaten beschreibt, die zur Verwirklichung auf das Internet angewiesen sind.

III. IuK-Kriminalität, Hightechkriminalität und Multimediale Kriminalität

Als weitere Begriffe sind die Informations- und Kommunikationstechnologie/IuK-Kriminalität und die Hightechkriminalität zu finden, die jedoch flächendeckend entweder implizit[67] oder gar explizit[68] mit Computerkriminalität, Internetkriminalität oder Cyberkriminalität gleichgesetzt werden.

Daneben ist *Vassilaki* der Auffassung, dass im Internet vermehrt neue Deliktsformen auftreten, die sich mit dem traditionellen Begriff der Computerkriminalität nicht mehr hinreichend genau beschreiben lassen, da das einzige gemeinsame Kriterium die missbräuchliche Nutzung von Datennetzen sei.[69] Unter Berücksichtigung soziologischer Komponenten zur Tätertypologie versucht sie sich daher an einem neuen Begriff und definiert „[…] Multimediale Kriminalität [als] jede gesetzwidrige und/oder ethisch verwerfliche Handlung im Zusammenhang mit dem Missbrauch der neuen Kommunikationstechniken und Medien, […]", sodass auch sie an Computer(netzwerke) als Tatwerkzeug anknüpft.

---

[66] *Koops*, Transnational Criminology Manual 2010, 735 (739), der sich dabei auf *Wall*, Cybercrime, S. 47 („true crimes wholly mediated by technology") bezieht.

[67] *Eisele*, Computer- und Medienstrafrecht, § 1 Rn. 1; *MacQuade*, Encyclopedia_of_Cybercrime, S. 44; *Sandywell*, in: Jewkes/Yar (Hrsg.), Handbook of Internet Crime, 38 (42 f.).

[68] KOM (2000) 890 endg., S. 13; KOM (2007) 267 endg., S. 2; *Kleve/Mulder/Noortwijk*, in: S. Kierkegaard/P. Kierkegaard (Hrsg.), Rights, duties & conflicts, S. 56 (59).

[69] *Vassilaki*, CR 1997, 297; unterstützend: *Barton*, Multimedia-Strafrecht, S. 24 ff.

IV. Technisch-informatische Definitionsansätze

Aus einem informatischen Blickwinkel stellen *Gordon/Ford* ein Zwei-Typen-Modell der Cyberkriminalität vor.[70] Anders als im Rahmen juristischer Auseinandersetzungen mit der Klassifikation von Kriminalitätsfeldern, stellen sie weniger auf die unterschiedlichen und gemeinsamen Modalitäten der Strafbarkeitsbegehung ab, sondern unterscheiden zwischen technikorientierter auf der einen und menschenorientierter Cyberkriminalität auf der anderen Seite. Technikorientierte Cyberkriminalität stütze sich in der Regel auf Schadsoftware zum Aufspüren von Systemschwachstellen und erschöpfe sich in einem singulären Angriff.[71] Sowohl die Charakteristika als auch die genannten Beispiele (Phishing, Datendiebstahl, Hacking) korrespondieren weitgehend mit der rechtlichen Kategorisierung von Cyberkriminalität mithilfe der Voraussetzung eines Computers bzw. Netzwerks als Angriffsobjekt. Menschenorientierte Cyberkriminalität zeichne sich hingegen regelmäßig durch mehrere Angriffsakte unter Missbrauch grundsätzlich unschädlicher Software (Kommunikationsprogramme, Webbrowser, File-Sharing-Plattformen) aus, sodass als Beispiele etwa Cyber-Stalking, Bestechung, Betrug, Finanzmarktmanipulationen und Betriebsspionage in Betracht kämen.[72] Auf rechtlicher Ebene bildet mithin die Kategorisierung von Cyberkriminalität anhand der Voraussetzung eines Computers oder Netzwerks als Begehungsmittel der Straftat ein passendes Äquivalent.

Noch stärker an der technischen Komponente einer Straftat orientiert, definieren *Turrini/Ghosh* Cyberkriminalität als eine Straftat, die durch den Angreifer unter erfolgreicher Kontrollübernahme über einen Computer oder über ein anderes technisches Gerät gegen oder ohne den Willen des rechtmäßigen Besitzers verübt wird,[73] was vermutlich das engste Verständnis darstellt.

Letztlich werden die Grenzen auch aus einem technischen Blickwinkel ganz ähnlich wie bei juristischen Abgrenzungsvorgängen gezogen. Insbesondere *Gorden/Ford* verdeutlichen, dass vor allem zwischen Straftaten, die ohne einen Computer oder ein Computernetzwerk gar nicht möglich wären, und Straftaten, die lediglich auch unter Nutzung eines Computer(netzwerk)s begangen werden können, Unterschiede bestehen. Demzufolge erscheint es also durchaus begründungsbedürftig, weshalb derartig verschiedene Deliktskategorien zu einem Kriminalitätsbereich zusammengefasst werden sollten.

---

[70] *Gordon/Ford*, J. Comp. Virol. 2006, 13 (14).
[71] *Gordon/Ford*, J. Comp. Virol. 2006, 13 (14).
[72] *Gordon/Ford*, J. Comp. Virol. 2006, 13 (14 f.).
[73] *Turrini/Ghosh*, in: dies. (Hrsg.), Cybercrimes, S. 3 (9).

C. Zusammenfassung

Mit den bislang vertretenen Ansätzen ist weder die Grenze des Computerkriminalitätsbegriffs in der Breite noch gegenüber verwandten Begrifflichkeiten herzustellen. Diese Schwierigkeit ist für sich genommen freilich weder ungewöhnlich noch grundsätzlich problematisch. Vielmehr ringen Praxis und Wissenschaft in vielen Gebieten um ein Verständnis der genutzten Begriffe um ihrer selbst willen. Überspitzt könnte man sagen, dass eine zweckfreie Forschung schließlich das Privileg einer jeden Wissenschaft sei.[74]

Für die Interpretation des Kriminalitätsbereichs der Computerkriminalität kann dies jedoch nicht gelten, da jenem durch Art. 83 Abs. 1 UAbs. 2 AEUV mittlerweile unionsrechtliche Relevanz – und damit ein Forschungszweck – dergestalt zukommt, dass die Definition darüber entscheidet, welche Straftaten von der strafrechtlichen Harmonisierungskompetenz der Europäischen Union erfasst sind. Die gezeigten Ansätze zur Begriffsbestimmung können insoweit allerdings lediglich gewisse Anhaltspunkte, nicht jedoch Konkretes liefern, sodass im Folgenden eine am Unionsrecht orientierte Auseinandersetzung mit dem Computerkriminalitätsbegriff im Querschnittsbereich zwischen Strafrecht, Verfassungsrecht und Europarecht vorgenommen wird.

§ 5 Die einzelnen Bereiche klassischer Begriffsbestimmungen

Wie bereits gezeigt, gehen die meisten klassischen juristischen Definitionen der Computerkriminalität (i. w. S.) von einem viergliedrigen Begriff aus, wie er auch in der Cybercrime Convention angelegt ist. Da diese vier Deliktsbereiche auch im Verlauf der Arbeit immer wieder herangezogen werden, werden sie im Folgenden kurz vorgestellt und zur Verdeutlichung jeweils anhand eines Straftatbestands illustriert.

A. Angriffe auf computergestützte Systeme

Dieser Deliktsbereich, auch als Computerkriminalität i. e. S. bezeichnet, ist mit dem 2. WiKG, bei dem sich der Gesetzgeber mit neuen kriminellen Erscheinungsformen unter Einbeziehung von Computern auseinandersetzt, ins StGB aufgenommen worden. Darunter fallen die §§ 202a, 202b, 202c, 303a und 303b StGB. Im Kern schützen diese Strafnormen die Vertraulichkeit (*confidentiality*),

---

[74] *Sieber*, in: GS Schlüchter (2002), S. 107 (108), Bezug nehmend auf *Constantinesco*, Rechtsvergleichung Bd. 2, S. 334 ff.; vgl. auch *Zweigert/Kötz*; Rechtsvergleichung, S. 12 ff.

Integrität (i*ntegrity*) und Verfügbarkeit (a*vailability*) von Computern und Computerdaten, weshalb sie häufig auch als „CIA-Delikte“ bezeichnet werden.[75]

Hacker H nutzt ein IT-Programm, um über das Internet und durch Überwindung technischer Zugangsschranken in das Computersystem des Unternehmens U einzudringen. Er kopiert daraufhin zunächst Daten des U auf seinen eigenen Computer und löscht schließlich die ursprünglichen Dateien auf den Servern des U.

Damit hat er den Tatbestand sowohl des Ausspähens von Daten nach § 202a StGB als auch der Datenveränderung nach § 303a StGB erfüllt.

B. Klassische Delikte unter Verwendung von Computern oder anderer moderner Endgeräte

Der Kategorisierung der Cybercrime Convention folgend stehen die klassischen oder auch computerbezogenen Delikte an zweiter Stelle. Sie beschreiben faktisch eine Art Auffangstrafbarkeit für Delikte unter Verwendung eines Computers, die von den spezifischeren Bereichen nicht hinreichend abgedeckt werden. Bei diesen Delikten entscheidet nicht das Tatobjekt oder die rechtsgutsbezogene Einordnung über den computerstrafrechtlichen Bezug, sondern eine wertende Gesamtbetrachtung.[76] Zu dieser Unterkategorie zählen vor allem der Computerbetrug nach § 263a StGB und die Verfälschung beweiserheblicher Daten gem. § 269 StGB.

Am Beispiel des Computerbetrugs lässt sich der Ausgangspunkt für eine solche Untergruppe von computerstrafrechtlichen Tatbeständen gut verdeutlichen. Der reguläre Betrugstatbestand des § 263 StGB erfasst lediglich die Täuschung einer Person, die daraufhin kausal einem Irrtum über Tatsachen unterliegt. Wenn allerdings ein Datenverarbeitungsmechanismus manipuliert (also „getäuscht“) wird, läuft zwar im Grundsatz ein ganz ähnlicher Prozess auf Seiten des Computerprogramms ab – es „irrt“. Da es sich aber nicht um eine Person, sondern um ein Computersystem handelt, ist eine Anwendung des § 263 StGB ausgeschlossen.[77] *Diese Lücke, die aufgrund des verfassungsrechtlichen Bestimmtheitsgrundsatzes (Art. 103 Abs. 2 GG) sowie des Analogieverbots für das Strafrecht nicht durch eine entsprechende Anwendung des § 263 StGB ge-*

---

[75] Statt vieler: *Gercke, M./Brunst*, Internetstrafrecht, Einl.

[76] *Gercke, M./Brunst*, Internetstrafrecht, Kap. 3 Rn. 159.

[77] Diese zu schließende Strafbarkeitslücke wird sowohl in der entsprechenden BT-Drs. 10/318, S. 16 ff., als auch in der Literatur umfangreich veranschaulicht; siehe u. a. *Bieber*r WM 1987, Beilage Nr. 6, 3 (21); *Heinz*, in: FS Maurer (2001), S. 1111 (1123); *Kolz*, wistra 1982, 167 (170).

schlossen werden kann, soll § 263a StGB füllen, der ebenfalls durch das 2. WiKG in das StGB eingefügt wurde.[78]

C. Inhaltsbezogene Delikte unter Verwendung von Computern oder anderer moderner Endgeräte

Den dritten computerstrafrechtlichen Bereich nach den gängigen Begriffskategorisierungen bilden die sog. inhaltsbezogenen Delikte. Darunter sind insbesondere die illegale Verbreitung (teilweise auch der Besitz) von (Kinder-)Pornografie und Äußerungsdelikte zu subsumieren. Inhaltsbezogene Delikte unter Verwendung von Computersystemen bringen die besondere Herausforderung mit sich, dass die Frage der Strafbarkeit weitgehend von den speziellen Moral- und Rechtsvorstellungen in den Nationalstaaten abhängt. Dies manifestiert sich beispielsweise im Spannungsfeld zwischen der deutschen Strafbarkeit der Holocaustleugnung oder der Verwendung von Symbolen verfassungswidriger Parteien und der US-amerikanischen Straffreiheit aufgrund der besonderen Betonung der Meinungsfreiheit in ähnlich gelagerten Fällen.[79] Vergleichbares ist auch bei Strafbarkeiten denkbar, die zum (vermeintlichen) Schutz religiöser oder ethischer Wertvorstellungen aufgestellt werden. Beispielhaft sei an dieser Stelle auf den Badawi-Fall aus Saudi-Arabien hingewiesen, bei welchem der Verurteilte durch die Veröffentlichung von Meinungen und Informationen auf einem Online-Blog gegen Strafgesetze des Landes verstoßen hatte.[80]

Diese Straftaten gewinnen ihre – vermeintlich – computerstrafrechtliche Dimension durch die Nutzung von Computer(systeme)n zur Verbreitung, zum Erwerb, zur Speicherung u. s. w. der strafrechtlich relevanten Inhalte.

D. Delikte gegen das Urheberrecht unter Verwendung von Computern oder anderer moderner Endgeräte

Neben den computerstrafrechtlichen Tatbeständen des StGB spielt im Nebenstrafrecht vor allem das Urheberstrafrecht eine maßgebliche Rolle im Bereich der Computerkriminalität. Ebenso wie die klassischen und inhaltsbezogenen Delikte, die unter Verwendung von Computersystemen begangen werden (kön-

---

[78] In der Literatur wird zumeist kritisiert, dass die Anlehnung an den regulären Betrugstatbestand dogmatisch misslungen sei, da der Computerbetrug untreue- und eigentumsbezogene Elemente enthalte, die dem § 263 StGB fremd seien. Die Beispielhaftigkeit als computerbezogenes Delikt schmälert diese Kritik freilich nicht.

[79] Vgl. *Gercke, M./Brunst*, Internetstrafrecht, Kap. 3 Rn. 256 f. m. w. N.

[80] *Wehrey*, Journal of Democracy 26.2 (2015), 71 (75).

nen), ist das Urheberstrafrecht grundsätzlich auch selbstständig und ohne computerstrafrechtliche Tatbestände relevant. Allerdings wächst seine Bedeutung durch Digitalisierung und Vernetzung von Medieninhalten stetig.[81] Dabei stellt das sanktionsrechtlich ausgestaltete Urheberstrafrecht eine Querschnittsmaterie zwischen Straf- und Zivilrecht dar. Dementsprechend sind die relevanten Straftatbestände in den §§ 106 ff. UrhG zivilrechtsakzessorisch formuliert.[82]

Exemplarisch ist die Vorschrift zur unerlaubten Verwertung urheberrechtlich geschützter Werke nach § 106 UrhG zu nennen. Danach ist derjenige mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bedroht, der ohne gesetzliche Lizenz[83] oder Einwilligung des Rechteinhabers ein Werk vervielfältigt (§ 16 UrhG), verbreitet (§ 17 UrhG) oder öffentlich wiedergibt (§ 15 Abs. 2 UrhG).[84]

§ 6 Problematik eines computerstrafrechtlichen Sammelbegriffs

Wissenschaftliche Arbeiten – zumindest der Rechtswissenschaft – beginnen regelmäßig mit einer Definition und ggf. einer Eingrenzung des Forschungsgegenstands. Dies ermöglicht es dem Autor, die Untersuchung zu fokussieren, um eine gewisse Tiefe gewährleisten zu können. Darüber hinaus macht er dadurch seine Untersuchung dem Leser gegenüber klar und verständlich und bietet hinreichend detaillierte Anknüpfungspunkte für qualifizierte Kritik, Zustimmung bzw. Weiterentwicklung. Bei der Bearbeitung von Thematiken zur Computer-, Internet- oder Cyberkriminalität kommt als weitere Herausforderung hinzu, dass weder in der Wissenschaft noch in der Praxis bisher eine allgemeingültige Definition für diese Kriminalitätsbereiche gefunden werden konnte, auf die sich der Bearbeiter stützen könnte.

Nachfolgend werden daher die unterschiedlichen Gesichtspunkte einer Begriffsbestimmung beleuchtet und insbesondere eine Bewertung vorgenommen, inwieweit die verschiedenen Aspekte mit den bisherigen Bemühungen um einheitliche Definitionen hinreichend bedient werden.

---

[81] *Gercke, M.*, ZUM 2007, 791 (793).

[82] Weiterführend zur Systematik der computerstrafrechtlichen und EU-rechtlichen Dimension des deutschen Urheberstrafrechts siehe *Dreier*, in: ders./Schulze (Hrsg.), Urheberrechtsgesetz, § 106 Rn. 1 ff.

[83] Gesetzliche Ausnahmen liegen beispielsweise vor bei § 69c Nr. 3 UrhG (veräußerte körperliche Vervielfältigungsstücke) und § 69d Abs. 2 UrhG (Sicherungskopien).

[84] *Hoeren*, Internetrecht, Stand: April 2016, S. 213 f. mit weiteren Hinweisen.

A. Begriffe als Beschreibung eines Kriminalitätsphänomens

Spätestens seit den 1990er-Jahren beschäftigen sich Studien, die regelmäßig durch internationale Organisationen in Auftrag gegeben wurden, intensiv mit dem Phänomen der (zu Beginn noch ausschließlich so betitelten) Computerkriminalität. Beispielsweise fertigte *Sieber* 1998 für die Europäische Kommission die „COMCRIME"-Studie an, *Kaspersen* 2009 die „Cybercrime and Internet Jurisdiction"-Studie für den Europarat, *Gercke* 2012 die „Understanding Cybercrime"-Studie für die ITU (International Telecommunication Union, eine Unterorganisation der Vereinten Nationen) sowie 2013 wiederrum *Sieber u. a.* die „Comprehensive Study on Cybercrime" für das United Nations Office on Drugs and Crime (UNODC). Diese Studien beschäftigen sich alle mit den jeweils aktuell besonders relevanten Erscheinungsformen des Kriminalitätsbereichs und machen Vorschläge zu deren Bekämpfung. Darüber hinaus legen sie alle einen besonders weiten Definitionsrahmen des Untersuchungsobjektes fest. Möglicherweise ist dieses Vorgehen darauf zurückzuführen, dass die Autoren sich einerseits nicht dem Vorwurf der Vernachlässigung eines im weiteren Verlauf relevanten Aspekts ausgesetzt sehen wollen. Andererseits wollten sie ggf. universellen Ansprüchen der Auftraggeber gerecht werden.

Da die internationalen Organisationen diese Studien in der Regel in Auftrag geben, um eine Grundlage für ihre zukünftigen Politiken zu haben bzw. diese damit begründen zu können, ist aus ihrer Sicht ein breit angelegter Forschungsgegenstand sinnvoll. Dass dabei Unschärfen im Detail auftreten können, spielt eine eher untergeordnete Rolle – es geht eher um die großen politischen Linien.

B. Verwendung in der polizeilichen und justiziellen Arbeit

In der polizeilichen und justiziellen Arbeit spielt in Deutschland insbesondere die jährlich erstellte Polizeiliche Kriminalitätsstatistik (PKS) eine Rolle. Sie enthält nahezu sämtliche bei der Polizei bekannt gewordenen und durch sie endbearbeiteten Straftaten.[85] Maßgebliche Aufgabe der PKS ist, neben einer statistischen Erfassung von Straftaten, vor allem die „Erlangung von Erkenntnissen für die vorbeugende und verfolgende Verbrechensbekämpfung, organisatorische Planungen und Entscheidungen sowie kriminologisch-soziologische Forschungen und kriminalpolitische Maßnahmen".[86]

---

[85] Nicht erfasst sind Staatsschutzdelikte, Verkehrsdelikte (mit Ausnahme der Verstöße gegen §§ 315, 315b StGB und § 22a StVG), Straftaten, die außerhalb der Bundesrepublik Deutschland begangen wurden, und Verstöße gegen strafrechtliche Landesgesetze, mit Ausnahme der einschlägigen Vorschriften in den Landesdatenschutzgesetzen.

[86] Polizeiliche Kriminalstatistik 2014, S. 1.

Bemerkenswert ist, dass die PKS Delikte einerseits nach dem Tatmittel Internet und andererseits nach dem Deliktsbereich Computerkriminalität und, sogar noch genauer, dem der IuK-Kriminalität i. e. S. aufschlüsselt.[87] Dabei zeigt die Differenzierung zwischen dem Tatmittel Internet – was letztlich nur auf die wenig bahnbrechende Erkenntnis hindeutet, dass sich Kriminelle bei der Tatbegehung moderner Technologien bedienen – und der Computerkriminalität bzw. IuK-Kriminalität i. e. S. ein Verständnis der Strafverfolgungsbehörden für die Diffizilität der Thematik und der Notwendigkeit einer differenzierten Betrachtung des Gesamtphänomens der Computer-, Internet- und Cyberkriminalität.

Das vom Europarat initiierte Projekt zum „European Sourcebook of Crime and Criminal Justice Statistics“[88] sowie die von den Vereinten Nationen verantworteten „UNODC Crime and Criminal Justice Statistics“[89] weisen keine gesonderte Strafbarkeitskategorie zur Computerkriminalität aus, sondern konzentrieren sich bislang auf klassische Straftaten und bilden globale Trends ab.

C. Tauglichkeit als Grundlage für internationale Harmonisierungen

Schließlich bleibt aber die Frage, ob die benannten Begriffsbestimmungen über ihre Tauglichkeit als Untersuchungsobjekte von Studien hinaus auch hinreichend bestimmt sind, um auch im Rahmen einer Kompetenznorm der Europäischen Union zur Harmonisierung des mitgliedstaatlichen Strafrechts Anwendung finden zu können.

Wie bereits weiter oben dargelegt, gibt Art. 83 Abs. 1 AEUV der Europäischen Union die Kompetenz zur Harmonisierung von Straftaten und Strafen in Bereichen besonders schwerer Kriminalität, die aufgrund einer grenzüberschreitenden Dimension eine besondere Notwendigkeit aufweisen, sie auf einer gemeinsamen Grundlage zu bekämpfen. Computerkriminalität stellt nach dem Willen der Vertragsgeber einen solchen Kriminalitätsbereich dar.

Bei der Untersuchung zum aktuellen Stand der Definitionsbemühungen zum Begriff der Computerkriminalität hat sich gezeigt, dass nach derzeitig herrschendem Verständnis, analog zur Cybercrime Convention, vier Deliktsgruppen adressiert werden. Das sind Straftaten, bei denen Computersysteme und -daten als Angriffsobjekte fungieren, Straftaten, bei denen Computer als Angriffs-

---

[87] Polizeiliche Kriminalstatistik 2014, S. 10 f.

[88] European Sourcebook of Crime and Criminal Justice Statistics 2014; abrufbar unter: http://www.heuni.fi/material/attachments/heuni/reports/qrMWoCVTF/HEUNI_report_80_European_Sourcebook.pdf (Stand: 07.08.2017).

[89] *Harrendorf/Heiskanen/Malby*, International Statistics on Crime and Justice 2010; abrufbar unter: https://www.unodc.org/documents/data-and-analysis/Crime-statistics/International_Statistics_on_Crime_and_Justice.pdf (Stand: 07.08.2017).

mittel bzw. Tatwerkzeuge eingesetzt werden, inhaltsbezogene Straftaten, bei denen Computer zur Verbreitung illegaler Inhalte eingesetzt werden, und schließlich Delikte, die sich mittels der Verwendung von Computern gegen das Urheberrecht richten. Dabei handelt es sich kaum flächendeckend um besonders schwere und typischerweise grenzüberschreitende Kriminalität. Im Folgenden werden daher die Konsequenzen dieser Feststellung, um den Begriff der Computerkriminalität i. S. d. Art. 83 Abs. 1 UAbs. 2 AEUV einzugrenzen.

§ 7 Begrenzende Auslegung des Computerkriminalitätsbegriffs

Die strafrechtliche Harmonisierungskompetenz nach Art. 83 AEUV wurde von Beginn an in der Strafrechtswissenschaft massiv kritisiert. Diese Kritik richtete sich einerseits gegen die angebliche Konzeptlosigkeit der europäischen Kriminalpolitik, die insbesondere dem Erfordernis eines legitimen Schutzzwecks, dem *Ultima-Ratio*-Prinzip, dem Schuld- und Bestimmtheitsgrundsatz (Gesetzlichkeitsgrundsatz) sowie dem Subsidiaritäts- und Kohärenzprinzip nicht hinreichend gerecht werde.[90] Neben dieser pauschalen, rein kriminalpolitischen Kritik, die in ähnlicher Weise auch gegenüber den meisten nationalen Kriminalpolitiken zu äußern wäre,[91] werden andererseits auch spezifisch europäische Zweifel, nämlich an der Legitimation der Europäischen Union zur Strafrechtsangleichung, vorgetragen. Weil das materielle Strafrecht das zentrale Herrschaftsinstrument einer Staatsgewalt darstelle, gefährde seine supranationale Angleichung Souveränität, Identität, Demokratie und Kultur und damit die Leitgedanken eines modernen Nationalstaats – ohne dass dem eine ausreichende demokratische Legitimation des Unionsgesetzgebers gegenüberstünde.[92]

Nun kann man diese Fundamentalkritik als Romantisierung des Nationalstaats und des Strafrechts abtun und stattdessen auf die zwingende Notwendigkeit der Rechtsangleichung zur transnationalen Verbrechensbekämpfung verweisen.[93] Diese Einschätzung vernachlässigt allerdings den Kern einer kritischen Begleitung europäischer Strafrechtssetzung, der im Folgenden am Beispiel des Harmonisierungsbereichs der Computerkriminalität freigelegt wird. Insbesondere wird dabei auf die tatsächlich vorherrschende Harmonisierungspraxis der

[90] *Asp u. a.* (Manifest Kriminalpolitik), ZIS 2009, 697 ff.

[91] *Vogel/Eisele*, in: Grabitz/Hilf/Nettesheim (Hrsg.), 57. EL Aug. 2015, Art. 83 AEUV Rn. 17; *Vogel*, in: Böse (Hrsg.), EnzEuR Bd. 9, § 7 Rn. 9.

[92] *Braum*, ZIS 2009, 418 ff. m. w. N.

[93] *Vogel/Eisele*, in: Grabitz/Hilf/Nettesheim (Hrsg.), 57. EL Aug. 2015, Art. 83 AEUV Rn. 19 ff.

Europäischen Union unter Beachtung der Voraussetzungen des Art. 83 AEUV, auf die Implikationen des Lissabon-Urteils des Bundesverfassungsgerichts und ihre Bedeutung im EU-rechtlichen Auslegungsprozess abzustellen sein, um schließlich einen einerseits europarechtlich beabsichtigten und gleichzeitig mitgliedstaatlich verfassungskonformen Begriff der Computerkriminalität zu bestimmen.

A. Voraussetzungen des Art. 83 Abs. 1 AEUV

Die Kompetenz der Europäischen Union zur strafrechtlichen Harmonisierung besteht nach Art. 83 Abs. 1 UAbs. 1 AEUV für Bereiche besonders schwerer Kriminalität mit gleichzeitig[94] grenzüberschreitender Dimension.

I. Besonders schwere Kriminalität

Die besondere Schwere eines Kriminalitätsbereichs ist empirisch und nicht ausschließlich normativ zu ermitteln, sodass nicht bereits die Möglichkeit ausreicht, sondern die tatsächliche Existenz einer Bedrohung für die Union nachgewiesen werden muss.[95] Kriterien zur Einordnung mithilfe einer gebotenen typisierenden Betrachtungsweise[96] seien etwa der Rang der geschützten Rechtsgüter sowie die Verletzungs- bzw. Gefährdungsintensität.[97]

Eine Legaldefinition des Begriffs der besonders schweren Kriminalität sieht das Unionsrecht nicht vor. Die Verträge arbeiten mit drei Abstufungen: „Kriminalität", „schwere Kriminalität" und „besonders schwere Kriminalität" – jeweils ohne eine gesetzliche Erläuterung dieser Begriffe.[98]

Art. 83 Abs. 1 UAbs. 2 AEUV zählt jedoch Kriminalitätsbereiche auf, die die Voraussetzungen nach UAbs. 1 erfüllen. Dabei wird einheitlich davon ausgegangen, dass alle aufgezählten Kriminalitätsbereiche – also auch die Computerkriminalität – automatisch und ohne eine weitere Prüfung unter die „besonders

---

[94] Statt aller bezüglich der Notwendigkeit des kumulativen Vorliegens der beiden Voraussetzungen: *Vogel/Eisele*, in Grabitz/Hilf/Nettesheim (Hrsg.), 57. EL Aug. 2015, Art. 83 AEUV Rn. 40.

[95] *Vogel/Eisele*, in: Grabitz/Hilf/Nettesheim (Hrsg.), 57. EL Aug. 2015, Art. 83 AEUV Rn. 41.

[96] Vgl. u. a. *Böse*, in: Schwarze (Hrsg.), Art. 83 AEUV Rn. 4.

[97] *Meyer*, in: von der Groeben/Schwarze/Hatje (Hrsg.), Art. 83 AEUV Rn. 13.

[98] Beispielsweise wird die Bekämpfung der „Kriminalität" als Unionsaufgabe im Rahmen des Raums der Freiheit, der Sicherheit und des Rechts in Art. 3 Abs. 2 EUV und in Art. 67 Abs. 3 AEUV genannt, während Art. 85 Abs. 1 AEUV, Art. 86 Abs. 4 S. 1 AEUV und Art. 88 Abs. 1 AEUV von „schwerer Kriminalität" sprechen. Zu den im EU-Primärrecht verwendeten Begrifflichkeiten siehe *Suhr*, in: Calliess/Ruffert (Hrsg.), Art. 83 AEUV Rn. 17.

schwerer Kriminalität“ i. S. d. Art. 83 Abs. 1 UABs. 2 AEUV fallen.[99] Auch wenn ein genannter Kriminalitätsbereich Bagatellfälle umfassen könne, ändere dies nichts an dessen Einordnung als Bereich „besonders schwerer Kriminalität“.[100] Diese rigorose Einteilung wird insbesondere beim Bereich der Computerkriminalität als problematisch gesehen.[101]

Die Tatsache, dass auch Bagatellfälle einem Bereich besonders schwerer Kriminalität unterfallen können, kann erklären, weshalb die auf Art. 83 Abs. 1 AEUV zurückgehenden EU-Rechtsakte teilweise sehr geringe Strafrahmengrenzen vorsehen.[102] Würde man diese (Bagatell-)Delikte individuell betrachten, wäre eine Harmonisierungsnotwendigkeit aufgrund besonderer Schwere jedenfalls nicht offensichtlich.

II. Grenzüberschreitende Dimension

Auch die grenzüberschreitende Dimension ist nicht für jedes Delikt einzeln zu prüfen. Im Rahmen des Art. 83 Abs. 1 AEUV reicht es für eine umfassende Harmonisierungskompetenz für den jeweiligen Kriminalitätsbereich aus, wenn dieser *typischerweise* von einer grenzüberschreitenden Dimension gekennzeichnet ist.[103] Objektive Kriterien zur Bestimmung einer grenzüberschreitenden Dimension sind dabei die Art der Straftat (z. B. bei Drogen-, Waffen- und Menschenhandel), deren Auswirkungen[104] (z. B. bei der Fälschung von Zahlungsmitteln in der Euro-Zone) oder eine besondere Notwendigkeit der Strafbarkeitsbekämpfung auf gemeinsamer Grundlage, die allerdings nicht bereits durch Bildung eines politischen Willens der Union begründet werden kann.[105] Vor allem das

---

[99] *Böse*, in: Schwarze (Hrsg.), Art. 83 AEUV Rn. 8; *Langbauer*, Das Strafrecht vor den Unionsgerichten, S. 94; *Vogel/Eisele*, in: Grabitz/Hilf/Nettesheim (Hrsg.), 57. EL Aug. 2015, Art. 83 AEUV Rn. 53; a. A. *Satzger*, in: Streinz (Hrsg.), Art. 83 AEUV Rn. 10; *Zimmermann*, JURA 2010, 844 (847).

[100] Vgl. *Vogel/Eisele*, in: Grabitz/Hilf/Nettesheim (Hrsg.), 57. EL Aug. 2015, Art. 83 AEUV Rn. 41; zustimmend *Tiedemann*, Wirtschaftsstrafrecht BT, Rn. 38.

[101] *Weigend*, ZStW 116 (2004), 275 (283).

[102] Art. 4 Abs. 4, Art. 5 Abs. 2–5 und Art. 6 Abs. 2 der Richtlinie 2011/93/EU (siehe im Einzelnen unten, Kap. 3 § 12 C.) sehen etwa lediglich Mindest-Höchststrafen von einem bzw. zwei Jahren vor.

[103] *Langbauer*, Das Strafrecht vor den Unionsgerichten, S. 94; *Vogel/Eisele*, in: Grabitz/Hilf/Nettesheim (Hrsg.), 57. EL Aug. 2015, Art. 83 AEUV Rn. 41; *Zöller*, in: FS Schenke (2011), S. 579 (588 f.).

[104] Für eine kritische Einordnung des Merkmals siehe *Meyer*, in: von der Groeben/Schwarze/Hatje (Hrsg.), Art. 83 AEUV Rn. 15, der auf das Fehlen eines Bezugspunkts für den Begriff der Auswirkungen hinweist.

[105] BVerfGE 123, 267 (410); *Böse*, in: Schwarze (Hrsg.), Art. 83 AEUV Rn. 5; *Meyer*, in: von der Groeben/Schwarze/Hatje (Hrsg.), Art. 83 AEUV Rn. 17.

Merkmal der besonderen Notwendigkeit ist nur schwerlich greifbar. Dabei muss, wenn es um den Schutz fundamentaler Werte und Rechtsgüter der EU und ihrer Mitgliedstaaten geht, dezidiert aufgezeigt werden, dass Kooperation und Koordination auf zwischenstaatlicher Ebene nicht ausreichen.[106]

In diesem Zusammenhang bemerkenswert ist, dass, sobald die grenzüberschreitende Dimension eines Kriminalitätsbereichs einmal erkannt und bestimmt ist, auch reine Inlandstaten von der Harmonisierungsermächtigung erfasst werden.[107] Dafür sprechen insbesondere gesetzessystematische Erwägungen. So führt Art. 86 Abs. 4 S. 1 a. E. AEUV, der die Erweiterung der Zuständigkeiten einer zu gründenden Europäischen Staatsanwaltschaft regelt,[108] explizit aus, dass diese auch im Falle von schwerer Kriminalität mit grenzüberschreitender Dimension nur dann gelten, wenn mehr als ein Mitgliedstaat von einer konkreten Straftat betroffen ist. Art. 83 Abs. 1 UAbs. 1 AEUV enthält diesen kleinen Zusatz indessen nicht. Im Umkehrschluss ist daher davon auszugehen, dass das Vorliegen einer typischerweise grenzüberschreitenden Dimension ausreichend zur Begründung der Harmonisierungskompetenz ist, sodass dann auch rein nationale Sachverhaltskonstellationen umfasst sind.

B. Reichweite der Harmonisierungskompetenz des Art. 83 Abs. 1 AEUV

Aus diesen beiden Feststellungen folgt, dass Art. 83 Abs. 1 AEUV die Europäische Union zur sog. umfassenden Harmonisierung eines Kriminalitätsbereichs ermächtigt. Es stellt sich allerdings die Frage, ob dennoch Beschränkungen der Harmonisierungskompetenz zu beachten sind.

I. Einschränkung der Kriminalitätsbereiche

Da die mit dem Vertrag von Lissabon in den AEUV aufgenommenen Kriminalitätsbereiche ohne weitere Prüfung als umfassend harmonisierungsfähig gelten,[109] wird im Allgemeinen davon ausgegangen, dass der Unionsgesetzgeber auch bei der Ausübung seiner Kompetenz die grenzüberschreitende Dimension einer Straftat, die einem der genannten Kriminalitätsbereiche unterfällt, nicht als Tatbestandsmerkmal aufnehmen müsse. Dies entspreche dem sog. Besitz-

---

[106] *Esser*, in: Zuleeg (Hrsg.), Europa als Raum der Freiheit, der Sicherheit und des Rechts, S. 25 (34).

[107] *Böse*, in: Schwarze (Hrsg.), Art. 83 AEUV Rn. 7; *Böse*, in: ders. (Hrsg.), EnzEuR Bd. 9, § 4 Rn. 9; *Meyer*, in: von der Groeben/Schwarze/Hatje (Hrsg.), Art. 83 AEUV Rn. 14; *Vogel/Eisele*, in: Grabitz/Hilf/Nettesheim (Hrsg.), 57. EL Aug. 2015, Art. 83 AEUV Rn. 44.

[108] Siehe zu dieser Thematik unten, Kap. 4 § 14 C.

[109] *Zöller*, in: FS Schenke (2011), 579 (587).

stand der Union.[110] Außerdem könne nur auf diese Weise „ein inkohärentes Nebeneinander von unangeglichenen Tatbeständen ohne grenzüberschreitende Dimension und angeglichenen Tatbeständen mit solcher Dimension“ vermieden werden.[111] Zu einer Begrenzung der Harmonisierungskompetenz auf rein transnationale Sachverhaltskonstellationen kommt es auf diesem Wege mithin nicht.

Hinsichtlich der grundsätzlich umfassenden Harmonisierungskompetenz für explizit genannte Rechtsbereiche ist der herrschenden Ansicht insoweit zuzustimmen, da eine Aufgliederung zwischen nationalen und transnationelen Tatbestandsalternativen die Rechtsanwendung maßgeblich erschweren würde. Gerade diese Tatsache allerdings führt zu einer besonderen Wichtigkeit der definitorisch klaren Umgrenzung der jeweiligen Kriminalitätsbereiche.[112] Andernfalls werden nicht nur im Zuge einer gebotenen unionsrechtlichen Harmonisierung auch rein nationale Sachverhalte mitgeregelt, sondern möglicherweise darüber hinaus zusätzliche, inhaltlich und thematisch verwandte, Strafbarkeitsbereiche indirekt einer schleichenden Vereinheitlichung unterzogen.

Um eine inhaltliche Konsistenz innerhalb der jeweiligen nationalen Strafrechtsordnung zu gewährleisten, könnten die Mitgliedstaaten versucht sein, auch analoge Rechtsbereiche den Harmonisierungsvorgaben des EU-Computerstrafrechts anzupassen. Als Beispiel sei insoweit auf das Urkundenstrafrecht verwiesen. Obwohl eine umfassende EU-Harmonisierungskompetenz diesbezüglich nach herrschender Ansicht nicht besteht,[113] *sind gegebenenfalls Strafbarkeitsanpassungen denkbar, um ein Auseinanderfallen von digitalen und analogen Verwirklichungsmodalitäten zu verhindern. Der Einfluss eines weit gefassten Kriminalitätsbereichs könnte sich somit noch einmal erheblich vergrößern.*[114]

[110] *Vogel/Eisele*, in: Grabitz/Hilf/Nettesheim (Hrsg.), 57. EL Aug. 2015, Art. 83 AEUV Rn. 44 unter Verweis auf die Rechtslage in den USA (Supreme Court of the United States, Urt. v. 26.4.1971 „Perez v. United States“, 402 U.S. 146). Besitzstand bedeutet an dieser Stelle, dass die Kompetenzzuweisung aufgrund eines Bereichs grenzüberschreitender Kriminalität im konkreten Einzelfall das Kriterium der grenzüberschreitenden Qualität dennoch nicht erfüllen muss. Wenn also ein Bereich als supranational regelungsbedürftig eingeordnet wird, unterfallen regelmäßig auch Inlandssachverhalte dieser Kompetenz.

[111] *Vogel/Eisele*, in: Grabitz/Hilf/Nettesheim (Hrsg.), 57. EL Aug. 2015, Art. 83 AEUV Rn. 44; vgl. auch *Weigend*, ZStW 116 (2004), 275 (283).

[112] Für den Bereich der Computerkriminalität ist dies eines der Kernanliegen dieser Arbeit, sodass insb. auf Kap. 2 § 8 D. verwiesen wird.

[113] *Vogel/Eisele*, in: Grabitz/Hilf/Nettesheim (Hrsg.), 57. EL Aug. 2015, Art. 83 AEUV Rn. 62.

[114] Siehe insoweit unten, Kap. 2 § 8 B.

II. Unklarer Wortlaut durch verschiedene Sprachfassungen

Andere Ansichten berufen sich hingegen auf eine andere Auslegung des Wortlauts der Norm. Aus der niederländischen Fassung des Art. 83 Abs. 1 UAbs. 2 AEUV („Het betreft de volgende vormen van criminaliteit …“) folge, dass auch für die bereits definierten Kriminalitätsbereiche eine Überprüfung anhand der beiden Kriterien möglich sei.[115] Die Vertreter dieser Argumentationslinie scheinen davon auszugehen, dass der Wortlaut der niederländischen Fassung durch seine Formulierung „betreft“ (zu Deutsch: betrifft) keine eindeutige und abschließende Einordnung der genannten Kriminalitätsbereiche als solche mit besonderer Schwere und typischerweise grenzüberschreitender Dimension zulasse. Vielmehr handele es sich eher um Regelbeispiele, welche die genannten Voraussetzungen im Anwendungsfall jeweils erneut zu erfüllen hätten.

Dabei ist die niederländische Fassung („betreft“) ein Sonderfall. Die übrigen Sprachfassungen (deutsch: „sind“, englisch: „are“, französisch: „sont“, spanisch: „son“) stützen die Sichtweise von einer feststehenden, unüberprüfbaren Liste von Kriminalitätsbereichen. Nur wenn ein neuer Kriminalitätsbereich nach Art. 83 Abs. 1 UAbs. 3 AEUV hinzukommen soll, muss eine Prüfung der Voraussetzungen des Art. 83 Abs. 1 UAbs. 1 AEUV erfolgen. Dementsprechend kann eine Begrenzung der Harmonisierungskompetenz auch nicht durch Einordnung der in Art. 83 Abs. 1 UAbs. 2 AEUV genannten Kriminalitätsbereiche als bloße Regelbeispiele statt als feststehende transnationale Kriminalitätsfelder mit besonderer Schwere gesehen werden.

III. Möglichkeit der Überprüfung konkreter Harmonisierungsmaßnahmen

Doch selbst die Vertreter dieser wortlautgetreuen Ansicht gehen regelmäßig davon aus, dass – auch wenn eine Überprüfung der Bereiche als solche ausgeschlossen sei – die Voraussetzungen der „besonderen Schwere“ und der „grenzüberschreitenden Dimension“ doch die Reichweite eines jeden genannten Kriminalitätsbereichs bestimmen würden und daher bei der Regelung konkreter Straftaten und Strafen zu berücksichtigen seien.[116] Demnach ist jede einzelne konkrete Maßnahme daraufhin zu überprüfen, ob sie nicht nur einem der ge-

---

[115] *Satzger*, in: Streinz (Hrsg.), Art. 83 AEUV Rn. 10; im Ergebnis ähnlich: *Zimmermann*, JURA 2010, 844 (847).

[116] *Böse*, in: Schwarze (Hrsg.), Art. 83 AEUV Rn. 8; *Böse*, in: ders. (Hrsg.), EnzEuR Bd. 9, § 4 Rn. 10; *Meyer*, in: von der Groeben/Schwarze/Hatje (Hrsg.), 83 AEUV Rn. 10; *Vogel/Eisele*, in: Grabitz/Hilf/Nettesheim (Hrsg.), 57. EL Aug. 2015, Art. 83 AEUV Rn. 53; siehe auch *Esser*, in: Zuleeg (Hrsg.), Europa als Raum der Freiheit, der Sicherheit und des Rechts, S. 25 (34 f.), der sich auf den wortgleichen Art. III-271 Abs. 1 UAbs. 2 des Europäischen Verfassungsentwurfs bezieht.

nannten Kriminalitätsbereich unterfällt, sondern ob die geregelten Sachverhaltskonstellationen auch selbst *typischerweise* eine besonders schwere Kriminalität darstellen und *typischerweise* eine grenzüberschreitende Dimension haben. Ein extensives Begriffsverständnis auf Ebene der Kompetenzbegründung wäre so gesehen auch aus einer Perspektive der Schonung nationaler Kompetenzen zu verkraften, da begrenzende Elemente in den Prozess der Kompetenzausübung einfließen.

Diese Auslegung würde insbesondere auch mit der Ansicht korrespondieren, dass Kompetenzkataloge ohnehin nicht an den Maßstäben des strafrechtlichen Bestimmtheitsgebots zu messen sind, da sie aufgrund ihrer Aufgabe im Rechtssystem mit echten Straftatbeständen nicht vergleichbar seien.[117] Folgerichtig hätte eine strikte Beachtung des Bestimmtheitsgrundsatzes daher erst auf zweiter und dritter Ebene im Rahmen des Sekundärrechtsakts bzw. dessen Umsetzung zu erfolgen. Der Begriff der Computerkriminalität wird allerdings bereits im Rahmen der Kompetenzvorschrift des Art. 83 Abs. 1 UAbs. 2 AEUV vereinzelt für auslegungsbedürftig gehalten, da er *zu* unklar sei.[118]

Zuzustimmen ist dieser Auffassung insoweit, als reinen Kompetenzkatalogen keinesfalls die Bestimmtheitsanforderungen eines Straftatbestands abverlangt werden können. Einerseits ist das auch insbesondere im europäischen Bereich überhaupt nicht nötig, da die primärrechtlichen Kompetenzen zunächst sekundärrechtlich in Richtlinien überführt und darüber hinaus mitgliedstaatlich umgesetzt werden müssen, sodass weitere Stufen auf dem Weg zu einer – den allgemeinen Bestimmtheitsanforderungen gerecht werdenden – Strafnorm zu nehmen sind.[119]

Andererseits muss aber auch eine Kompetenznorm, vor allem dann, wenn sie besonders sensible Bereiche wie das Strafrecht betrifft, zumindest erkennen lassen, welche Deliktsgruppen harmonisiert werden können. Rechtsnormen müssen für den Adressaten verständlich sein. Freilich ist es insbesondere bei einem offenen Verfassungstext, wie dem EU-Primärrecht, nicht erforderlich, dass bereits der Wortlaut einer Norm dem Adressaten ein unmittelbares Ver-

---

[117] *Bacigalupo*, ZStW 116 (2004), 326 (329); *Kretschmer*, in: Vedder/Beutel (Hrsg.), Europäischer Verfassungsvertrag, Art. III–271 Rn. 7; *Tiedemann*, Wirtschaftsstrafrecht BT, Rn. 43; *Walter*, ZStW 117 (2006), 912 (927 f.), die sich zwar teilweise noch auf die gescheiterte Europäische Verfassung beziehen, was allerdings aufgrund der Wortgleichheit der Harmonisierungskompetenzen im Strafrecht zum AEUV unbedenklich für die Argumentation ist.

[118] *Walter*, ZStW 117 (2006), 912 (928).

[119] Auch *Meyer*, in: von der Groeben/Schwarze/Hatje (Hrsg.), Art. 83 AEUV Rn. 10 weist auf die abgestuften Bestimmtheitsanforderungen zwischen Kompetenzvorschrift, Richtlinie und nationalem Umsetzungsgesetz hin.

ständnis des Inhalts vermittelt; dennoch sind gewisse Mindestanforderungen an die Kontinuität und relative Vorhersehbarkeit des Norminhalts zu stellen.[120]

In Art. 83 Abs. 1 AEUV ist dabei vor allem die Kategorie der Computerkriminalität problematisch. Aus dem Wortlaut („Derartige Kriminalitätsbereiche *sind* …“ [Hervorhebung des Verf.]) ist nicht ersichtlich, weshalb die Voraussetzungen der „besonderen Schwere“ und der „grenzüberschreitenden Dimension“ im Zuge des sekundärrechtlichen Verfahrens abermals zur Prüfung der geplanten Richtlinie herangezogen werden sollten, wenn deren positives Vorliegen doch bereits primärrechtlich verankert ist. Als Begrenzungsmechanismen fungieren daher lediglich die allgemeinen Kompetenzbegründungs- und -ausübungsschranken des EU-Primärrechts.[121] Auch die tatsächliche Praxis beim Erlass von Richtlinien nach Art. 83 Abs. 1 AEUV spricht gegen das Erfordernis einer Überprüfung des jeweiligen Sekundärrechtsakts auf die „besondere Schwere“ und „grenzüberschreitende Dimension“ der betroffenen Straftaten. Wie im weiteren Verlauf dieser Arbeit noch nachgewiesen wird,[122] umfassen die strafrechtlichen EU-Richtlinien auch flächendeckend solche Straftaten, die sich mit Strafrahmen von bis zu einem Jahr o. ä. kaum unter den Begriff der besonders schweren Kriminalität subsumieren lassen.[123] Richtigerweise ist damit sowohl nach dem Wortlaut der Vorschrift als auch dem offenkundigen Verständnis der EU-Institutionen davon auszugehen, dass die Kriminalitätsbereiche des Art. 83 Abs. 1 UAbs. 2 AEUV abschließend als besonders schwer und mit grenzüberschreitender Dimension definiert sind und eine Harmonisierung somit grundsätzlich unabhängig von einer Subsumtion der einzelnen Straftat unter die Voraussetzungen des Art. 83 Abs. 1 AEUV erfolgen kann.

Um dennoch nicht einer grenzen- oder uferlosen Kompetenznorm gegenüberzustehen, ist mithin auf der Primärrechtsebene eine eigene Auslegung des Begriffs der Computerkriminalität notwendig, die im Folgenden vorgenommen wird. An dieser Stelle zeigen dann auch die Voraussetzungen der besonderen Schwere und der grenzüberschreitenden Dimension ihre begrenzende Funktion. Zwar können die einzelnen Rechtsakte nicht unionsrechtskonform hinsichtlich ihrer „besondere Schwere“ und „grenzüberschreitende Dimension“ überprüft werden, jedoch ist dies auch dann nicht nötig, wenn das Begriffspaar stattdessen bereits zur Auslegung des primärrechtlichen Begriffs der Computerkriminalität (oder ggf. auch jedes anderen in Art. 83 Abs. 1 UAbs. 2 AEUV aufgeführten Kriminalitätsbereichs) herangezogen wird. Nach hier vertrenener Auffassung kann mithin nur

---

[120] *Hahn-Lorber*, ECJ 2010, 760 (778).
[121] Siehe unten, Kap. 2 § 7 D.
[122] Siehe unten, Kap. 3 § 12 C.
[123] Das Gleiche gilt für die grenzüberschreitende Dimension, die in keinem der Fälle Tatbestandsvoraussetzung ist.

dasjenige Verständnis des Computerkriminalitätsbegriffs primärrechtmäßig sein, das diesen beiden Voraussetzungen gerecht wird. Die Einbeziehung der beiden Voraussetzungen des Art. 83 Abs. 1 AEUV in die Auslegung des Begriffs ist an dieser Stelle auch zwingend, da sie ansonsten für den UAbs. 2 wertlos wären und nur hinsichtlich Art. 83 Abs. 1 UAbs. 3 AEUV relevant würden.

Nicht die Überprüfung von Sekundärrechtsakten, sondern allein die Auslegung der Kriminalitätsbereiche des Art. 83 Abs. 1 UAbs. 2 AEUV anhand der Voraussetzungen „besondere Schwere" und „grenzüberschreitende Dimension" sichert somit eine rechtmäßige Strafrechtsharmonisierung. Im Folgenden wird daher untersucht, welche Auslegungsoptionen für den Computerkriminalitätsbegriff bestehen.

C. Auslegung des Computerkriminalitätsbegriffs gem. Art. 83 Abs. 1 AEUV

Zu den strafrechtlichen Kompetenzvorschriften des EU-Primärrechts hat das Bundesverfassungsgericht in seinem Lissabon-Urteil detailliert Stellung genommen. Dabei hat es diesbezüglich eine restriktive Auslegung gefordert, da straf- und strafverfahrensrechtliche Normen die demokratische Selbstbestimmung besonders empfindlich berühren.[124]

Zur Beurteilung der Vorgaben des Bundesverfassungsgerichts wird einerseits die Frage des Rangverhältnisses zwischen europäischem und mitgliedstaatlichem Recht geklärt[125] und andererseits auf die Methoden zur Auslegung des europäischen Primär- und Sekundärrechts eingegangen,[126] bevor anschließend eine Auseinandersetzung mit den strafrechtlichen Implikationen des Lissabon-Urteils des Bundesverfassungsgerichts erfolgt.[127]

I. EU-Recht vs. nationales Recht: Rangverhältnis und Auslegungsmethodik

Obwohl die europäischen Verträge völkerrechtlichen Ursprungs sind, handelt es sich bei dem durch sie geschaffenen Recht um eine eigenständige, unmittelbar geltende Rechtsordnung.[128] Im Unterschied zum Völkerrecht, das erst durch einen jeweiligen nationalen Umsetzungsakt innerstaatlich verbindlich und auch erst in diesem Rahmen in die nationale Normenhierarchie eingeordnet wird,[129]

[124] BVerfGE 123, 267 (410).

[125] Siehe sogleich, Kap. 2 § 7 C. I. 1.

[126] Siehe unten, Kap. 2 § 7 C. I. 2.

[127] Siehe unten, Kap. 2 § 7 C. II.

[128] Statt aller: *Borchardt*, Grundlagen, § 4 Rn. 129 f.

[129] Dabei ist ein breites Spektrum zur Einordnung möglich, sodass inkorporiertes Völkerrecht, das innerstaatlich dem nationalen Verfassungsrecht vorgeht, zwischen Verfassungs-

stellt sich die Frage der Hierarchie zwischen EU-Recht und nationalem Recht umso mehr.[130]

1. Vorrang des Unionsrechts

Da die Europäische Union lediglich eine Rechtsgemeinschaft und kein selbstständiger Staat ist, hat sie neben dem Recht selbst keine weiteren Durchsetzungsmechanismen. Daher ist die vorrangige Geltung des Unionsrechts gegenüber mitgliedstaatlichem Recht unerlässlich.[131] Bereits 1964 stellte der EuGH in der Rechtssache „Costa/ENEL“[132] den Anwendungsvorrang des Unionsrechts gegenüber jedem entgegenstehenden mitgliedstaatlichen Recht, also auch gegenüber (Verfassungs-)Recht, fest. Die Mitgliedstaaten hätten Hoheitsrechte endgültig auf die Europäische Union übertragen, die eine eigene Rechtsordnung darstelle. Diese Rechtsordnung könnten sie nicht durch spätere, einseitige, mit dem Unionsbegriff unvereinbare Maßnahmen rückgängig machen. Vielmehr müsse das Unionsrecht, im gesamten Bereich der EU, einheitlich und vollständig gelten.[133] Zumindest inzident findet sich dieser Grundsatz des Anwendungsvorrangs auch in Art. 4 Abs. 3 EUV. Danach haben die Mitgliedstaaten sämtliche Maßnahmen, welche die Verwirklichung der Unionsziele gefährden könnten, zu unterlassen.

a. Rechtsfolge des Vorrangs

Aus der genannten Vorrangregel, die rechtstheoretisch streng genommen eigentlich eine Kollisionsregel ist,[134] ergibt sich, dass dem europäischen Recht widersprechendes mitgliedstaatliches Recht unanwendbar ist. Damit ist letztlich eine Verdrängung oder Überlagerung des nationalstaatlichen Rechts gemeint,[135] ohne dass dies allerdings zu dessen Nichtigkeit führen würde.[136] Auch wenn es sich im Grundsatz lediglich um eine politische Unterscheidung handelt, um eine behutsame europäische Integration zu ermöglichen, ist die Differenzierung zwischen Unanwendbarkeit und Nichtigkeit einerseits für theoretisch denkbare

---

recht und einfachem Gesetzesrecht oder lediglich auf der Stufe einfachen Gesetzesrechts stehen kann.

[130] *Borchardt*, Grundlagen, § 4 Rn. 141 ff.

[131] Statt aller: *Epiney*, in: Bieber/ders./Haag (Hrsg.), Europäische Union, § 2 Rn. 65 ff.

[132] EuGH, Rs. 6/64 , Slg. 1964, 1251 ff. – *Costa/E.N.E.L.*

[133] *Borchardt*, Grundlagen, § 4 Rn. 144 f.

[134] Siehe dazu *Funke*, DÖV 2007, 733 (738).

[135] *Hahn-Lorber*, ELJ 2010, 760 (764) m. w. N.; *Nettesheim*, in: Oppermann/Classen/ders. (Hrsg.), Europarecht, § 10 Rn. 32.

[136] Zumindest früher wurde jedoch, etwa in der Dissertation von *Grabitz*, Gemeinschaftsrecht bricht nationales Recht, auch diese Auffassung vertreten.

Fälle eines Außerkrafttretens von Unionsrecht relevant, da das unanwendbare mitgliedstaatliche Recht dann wieder aufleben würde, und andererseits für solche Sachverhalte bedeutsam, die nicht vom EU-Recht erfasst werden.[137]

b. Reaktion auf mitgliedstaatlicher Ebene

Obgleich nationale Gerichte mit dieser Vorrangregel zunächst fremdelten,[138] besteht heutzutage über deren Anerkennung Einigkeit.[139] Für die Bundesrepublik Deutschland ist in diesem Zusammenhang der Beschluss des Zweiten Senats des Bundesverfassungsgerichts vom 6. Juli 2010 maßgeblich, der folgende Aussage beinhaltet: „Das Recht der Europäischen Union kann sich nur wirksam entfalten, wenn es entgegenstehendes mitgliedstaatliches Recht verdrängt. […] Im Anwendungsbereich des Unionsrechts ist entgegenstehendes mitgliedstaatliches Recht grundsätzlich unanwendbar. Der Anwendungsvorrang folgt aus dem Unionsrecht, weil die Union als Rechtsgemeinschaft nicht bestehen könnte, wenn die einheitliche Wirksamkeit des Unionsrechts in den Mitgliedstaaten nicht gewährleistet wäre.“[140] Damit akzeptiert das Bundesverfassungsgericht sowohl den Anwendungsvorrang des EU-Rechts als auch die Auslegungshoheit des EuGH bezüglich der Europäischen Verträge.

Allerdings findet sich in der Rechtsprechung des Bundesverfassungsgerichts auch immer wieder eine Betrachtungsweise, die den Mitgliedstaaten die „Herrschaft über die Verträge“ sichern soll.[141] Besonders deutlich wird dieser scheinbare Widerspruch bei der Auslegung unionsrechtlicher Kompetenznormen. So ist beispielsweise die Auslegung des Computerkriminalitätsbegriffs von unmittelbarer Bedeutung für auf Art. 83 AEUV beruhende Richtlinien. Sollte die Vereinbarkeit eines solchen Rechtsaktes mit dem Primärrecht infrage stehen, geht der EuGH davon aus, selbstständig und ausschließlich über diese Rechtsfrage entscheiden zu können. Diesen Ansatz erkennt das Bundesverfassungsgericht, wie oben gezeigt, auch an, behält sich durch die sog. *Ultra-vires*-Kontrolle allerdings eine Letztentscheidungskompetenz in verfassungsrechtlich besonders sensiblen Fragen vor. Aufgrund der mehrfach zitierten besonderen Bedeutung des Strafrechts für die nationale Identität eines Mitgliedstaats ist die erstmalige Anwendung dieses Verfahrens oder zumindest dessen Androhung im

---

[137] *Borchardt*, Grundlagen, § 4 Rn. 145; *Nettesheim*, in: Oppermann/Classen/ders. (Hrsg.), Europarecht, § 10 Rn. 32.

[138] Weitere Ausführungen zur mitgliedstaatlichen Rechtsprechung in der Vorrangfrage finden sich bei *Bieber*, in: ders./Epiney/Haag (Hrsg.), Die Europäische Union, § 3 Rn. 39 f.

[139] *Borchardt*, Grundlagen, § 4 Rn. 146.

[140] BVerfGE 126, 286 (301).

[141] Einen Überblick zum Stand der Rechtsprechung des BVerfG erarbeitet *Polzin*, JuS 2012, 1 ff.

Bereich von Art. 83 AEUV nicht unwahrscheinlich, sodass ein kurzer Überblick geboten ist.

Die *Ultra-vires*-Kontrolle (Doktrin vom sog. ausbrechenden Rechtsakt) aus seinem „Maastricht-Urteil" konkretisiert das Bundesverfassungsgericht in o. g. Beschluss. Das Bundesverfassungsgericht sei danach verpflichtet, „Handlungen der europäischen Organe und Einrichtungen darauf zu überprüfen, ob sie aufgrund ersichtlicher Kompetenzüberschreitungen oder aufgrund von Kompetenzausübungen im nicht übertragbaren Bereich der Verfassungsidentität (Art. 79 Abs. 3 GG) erfolgen". Die *Ultra-vires*-Kontrolle lässt den Anwendungsvorrang des Unionsrechts grundsätzlich unberührt. Das Bundesverfassungsgericht behält sich vielmehr vor, einer selbstständigen Vertragsänderung oder einer eigenständigen Kompetenzausweitung durch die Europäische Union Einhalt zu gebieten. Infolge der grundsätzlichen Anerkennung des Vorrangs ist die *ultra-vires*-Kontrolle allein durch das Bundesverfassungsgericht und darüber hinaus zurückhaltend und europarechtsfreundlich auszuüben.[142]

Neben dem Bundesverfassungsgericht haben sich aus Anlass des Lissabon-Vertrags[143] auch weitere mitgliedstaatliche Verfassungsgerichte mit dem Einfluss der europäischen Integration auf die Staatlichkeit der Nationalstaaten beschäftigt.[144] Im Zentrum der akademischen Aufmerksamkeit standen dabei die jeweiligen Urteile des tschechischen,[145] des polnischen[146] und des französischen[147] Verfassungsgerichts. Besonders relevant war jeweils die Frage nach einem etwaigen Souveränitätsverlust. Auch wenn die Ansätze aufgrund der jeweils unterschiedlich ausgestalteten nationalen Verfassungstexte variieren, kamen letztlich all diese Gerichte zu dem Schluss, dass die Souveränität der Nationalstaaten auch nach dem Vertrag von Lissabon ausreichend gewährleistet ist.

---

[142] Vgl. *Borchardt*, Grundlagen, § 4 Rn. 146.

[143] BVerfGE 123, 267 ff.; siehe dazu insb. unten, Kap. 2 § 7 C. II.

[144] Siehe dazu weiterführend *Theil*, GLJ 2014, 599 ff.

[145] Czech CC, case Pl ÚS 19/08, Urteil v. 26.11.2008 – *Lissabon I*, eine englische Übersetzung findet sich unter: http://www.usoud.cz/en/decisions/?tx_ttnews%5Btt_news%5D=484&cHash=621d8068f5e20ecadd84e0bae0527552 (Stand: 07.08.2017) und Czech CC, case Pl ÚS 29/09, Urteil v. 3.11.2009 – *Lissabon II*, ein englische Übersetzung findet sich unter: http://www.usoud.cz/en/decisions/?tx_ttnews%5Btt_news%5D=466&cHash=eedba7ca14d226b879ccaf91a6dcb276 (Stand: 07.08.2017).

[146] Trybunał Konstytucyjny [Constitutional Tribunal], Urteil v. 24.11.2010– Ref. No. K 32/09, eine englische Übersetzung findet sich in *Budziło*, Rulings of the Constitutional Court, S. 192 ff.

[147] Décision n° 2007-560 DC du 20 décembre 2007, Recueil, p. 459 – Journal officiel du 29 décembre 2007, page 21813, texte n° 96; eine deutsche Übersetzung findet sich unter: http://www.conseil-constitutionnel.fr/conseil-constitutionnel/root/bank_mm/allemand/2007560dc.pdf (Stand: 07.08.2017).

Obwohl diese Verfassungsgerichte sich, anders als das Bundesverfassungsgericht, eine *Ultra-vires*-Kontrolle nicht ausdrücklich vorbehalten haben, sind in den Urteilen des tschechischen und des polnischen Verfassungsgerichts doch vergleichbare Elemente zu erkennen. Das tschechische Verfassungsgericht etwa behält sich das Recht vor, die konstitutionelle Ordnung zu verteidigen, indem in außergewöhnlichen Fällen Rechtsakte der EU darauf hin überprüft werden, ob sie über die durch die Tschechische Republik übertragenen Kompetenzen hinausgehen.[148] Ein ausdifferenziertes *Ultra-vires*-Verfahren kann darin freilich nicht erkannt werden, sodass es vielmehr als Warnung zu verstehen ist. Das polnische Verfassungsgericht hatte bereits zuvor die Durchführung eines *Ultra-vires*-Verfahrens angedroht.[149] In seiner Lissabon-Entscheidung hat es das Gericht dann allerdings bei der Andeutung belassen, dass es, sollte die EU die legislativen Rechte der Polnischen Republik verfassungswidrig einschränken, einschreiten werde.[150] Das französische Verfassungsgericht hingegen hat sich in seiner Lissabon-Entscheidung nicht zur Problematik des Verstoßes eines Sekundärrechtsakts gegen nationales Verfassungsrecht geäußert. Das liegt laut *Theil* vor allem daran, dass europäische Primärrechtsänderungen regelmäßig in die französische Verfassung aufgenommen werden und so eine Kollision mit Sekundärrechtsakten faktisch ausgeschlossen wird.[151]

Abgesehen von diesem recht radikalen französischen Ansatz, der die Prüfung der Vereinbarkeit von EU- und nationalem Recht auf die Ebene der Primärrechtsänderung vorverlagert und damit in der Konsequenz ausschließlich den EuGH in der Auslegungsverantwortung sieht, ist durchaus eine Tendenz in der europäischen Verfassungsrechtsprechung zur *Ultra-vires*-Kontrolle zu erkennen. Zwar sind die Verfahren dazu entweder noch nicht ausgearbeitet oder mit hohen Hürden ausgestattet,[152] die Überprüfung der Vereinbarkeit von Sekundärrechtsakten mit dem jeweiligen nationalen Verfassungsrecht haben die europäischen Verfassungsgerichte jedoch zumindest für Ausnahmefälle nicht aus der Hand gegeben.

Es stellt sich also wegen der vielfach beschworenen Relevanz des Strafrechts als Kernelement eines Staats auch und sogar insbesondere im Rahmen einer strafrechtlichen Arbeit die Frage nach der Auslegungssystematik und -methodik von unionsrechtlichen Kompetenzregeln. Sind diese im Sinne eines „genuin

---

[148] Czech CC, case Pl ÚS 19/08, Urteil v. 26.11.2008, Rn. 139 – *Lissabon I.*

[149] Trybunał Konstytucyjny [Constitutional Tribunal], Judgment of 11 May 2005 – Ref. No. K 18/04 – *Budziło*, Rulings of the Constitutional Court, S. 59 Rn. 15.

[150] *Theil*, GLJ 2014, 599 (628 f.).

[151] *Theil*, GLJ 2014, 599 (629).

[152] *Möllers*, EuConst 2011, 161 (166).

europarechtlichen" Ansatzes,[153] wie ihn die EU-Institutionen vertreten, auszulegen und wenn ja, wie sieht ein solcher Auslegungsvorgang aus? Oder gibt es zumindest in besonders verfassungsrelevanten Aspekten eine Letztentscheidungs- und damit Letztauslegungskompetenz der nationalen Verfassungsgerichte, wie sie im Gedanken zur *Ultra-vires*-Kontrolle anklingen?

2. Auslegungsmethodik im EU-Primärrecht

Durch die Emanzipation von seinen völkerrechtlichen Ursprüngen hat sich das EU-Recht eine Eigenständigkeit erarbeitet, die sich nicht lediglich im Rangverhältnis zwischen Völkerrecht und nationalstaatlichem (Verfassungs-)Recht ausdrückt, sondern darüber hinaus auch eine eigene unionsrechtliche Interpretationslehre hervorgebracht hat.[154] Diese orientiert sich zwar grundsätzlich an den bekannten juristischen Auslegungsmethoden, akzentuiert und erweitert deren Gewichtung jedoch selbstständig aus unionsrechtlicher Perspektive.[155] Dabei beruht sie auch nicht auf den völkerrechtlichen Auslegungsgrundsätzen,[156] wie sie im sog. Recht der Verträge niedergelegt sind.[157]

Es wird erstens zu zeigen sein, dass die klassische juristische Hermeneutik, die bereits im nationalen Verfassungsrecht regelmäßig an ihre Grenzen stößt, im unionsrechtlichen Kontext für sich alleine genommen keine hinreichende Auslegungsmethodik darstellt, sondern lediglich als Grundlage im Interpretationsprozess herangezogen werden kann.[158]

Zweitens werden methodische Erweiterungen dargelegt[159] und unter Rückgriff auf das Bild des Verfassungsgerichtsverbunds[160] verdeutlicht, dass trotz weithin akzeptierter Auslegungshoheit des EuGH bezüglich des EU-Rechts auch die mitgliedstaatlichen Verfassungsgerichte als Akteure im europäischen Auslegungsprozess auftreten und ihre Entscheidungen einen maßgeblichen Anteil am Auslegungsergebnis haben.[161]

---

[153] *Nettesheim*, in: Oppermann/Classen/ders. (Hrsg.), Europarecht, § 10 Rn. 5.

[154] *Nettesheim*, in: Oppermann/Classen/ders. (Hrsg.), Europarecht, § 9 Rn. 165 ff.; weitergehende Nachweise dazu finden sich bei *Pechstein/Drechsler*, in: Riesenhuber (Hrsg.), Europäische Methodenlehre, § 7 Rn. 11 ff.

[155] *Müller/Christensen*, Juristische Methodik Bd. 2 – Europarecht, S. 27.

[156] *Everling*, JZ 2000, 217 (223); *Wieland*, NJW 2009, 1841 (1843).

[157] Die Auslegungsregeln für völkerrechtliche Verträge sind in den Art. 31–33 des Wiener Übereinkommens über das Recht der Verträge (WÜRV) v. 23.5.1969 niedergelegt; für weitergehende Hinweise: statt vieler: *Villiger*, Vienna Convention, Sec. 3 Art. 31–33.

[158] Siehe insoweit sogleich, Kap. 2 § 7 C. I. 2. a.

[159] Siehe unten, Kap. 2 § 7 C. I. 2. a.

[160] *von Danwitz*, in: Hatje/Müller-Graff (Hrsg.), EnzEuR Bd. 1, § 13 Rn. 34 ff.; *Voßkuhle*, NVwZ 2010, 1.

[161] Siehe unten, Kap. 2 § 7 C. I. b. cc.

Schließlich werden drittens die Verlautbarungen des BVerfG im Lissabon-Urteil zur Auslegung des Art. 83 AEUV auf ihre dogmatische Validität hin untersucht und in den gesamten europäischen Auslegungsprozess eingeordnet.[162]

a. Grundlagen des europäischen Auslegungsvorgangs

Die Grundlage eines jeden juristischen Auslegungsvorgangs stellt die klassische juristische Hermeneutik mit ihren vier, auf *von Savigny* zurückgehenden Kanones dar.[163] Dabei wird seit jeher bestritten, dass die sog. klassisch-hermeneutische Methode bei der Verfassungsinterpretation hinreichende Ergebnisse erzielen kann, weshalb auch im innerstaatlichen Verfassungskontext verschiedene (ergänzende) Methoden herangezogen werden.[164] Dies muss umso mehr innerhalb der Europäischen Union gelten: Zunächst ist die EU nicht (bundes-)staatlich, sondern als Staatenverbund mit unterschiedlichen Verfassungen und Verfassungstraditionen ausgestaltet. Die Europäischen Verträge als dessen Grundlage sind überdies quasi-verfassungsrechtlich ausgestaltet. Schließlich gibt es mit dem EuGH eine einem „Verfassungsgericht der Europäischen Union" zumindest stark angenäherte Instanz, die die Auslegung des Unionsrechts überwacht.[165] Diese Faktoren sprechen dafür, sowohl die klassische Hermeneutik um genuin verfassungsrechtliche Auslegungsmethoden zu erweitern als auch punktuell noch weitergehende Interpretationsmethoden anzuwenden. Nur so ist den Besonderheiten des EU-Rechts gegenüber klassischem Gesetzesrecht und sogar gegenüber nationalstaatlichen Verfassungen gerecht zu werden.

Die klassisch-juristische Hermeneutik verfolgt, vereinfacht ausgedrückt, das Ziel, ein bereits existentes Interpretationsergebnis zu finden, indem ein starres Auslegungskorsett herangezogen wird.[166] Es handelt sich dabei, unabhängig von der jeweiligen methodischen Strömung, letztlich immer um einen Versuch,

---

[162] Siehe unten, Kap. 2 § 7 C. II.

[163] *von Savigny*, System des römischen Rechts, Bd. 1, S. 212 ff., wobei laut *Böckenförde*, NJW 1976, 2089 (2090) Fn. 9, interessant sei, dass die teleologische Auslegungsmethode bei *von Savigny* noch keine eigenständige Rolle eingenommen hat.

[164] Einen wegweisenden Überblick dazu bietet *Böckenförde*, NJW 1976, 2089 ff.; vgl. auch *Häberle*, JZ 1989, 913 ff.

[165] *Iglesias*, in: Walter-Hallstein-Institut für Europa (Hrsg.), Europäische Verfassung in der Krise, S. 107 (110 f.); *Häberle/Kotzur*, Europäische Verfassungslehre, S. 778 ff.; *Mayer*, in: von Bogdandy/Bast (Hrsg.), Europäisches Verfassungsrecht, S. 559 ff.; *Voßkuhle*, NVwZ 2010, 1 (3).

[166] Ob es eine Rangfolge der vier Kanones gibt, ist seit jeher umstritten, *von Savigny*, System des römischen Rechts, Band 1, S. 212, jedenfalls geht nicht davon aus. Zum Rangfolgestreit aus verfassungsrechtlicher Sicht siehe u. a. *Gern*, Die Rangfolge der Auslegungsmethoden von Rechtsnormen, Verwaltungs-Archiv 80 (1989), 415 (430 ff.); *Hassold*, in: FS Larenz II (1983), S. 211 (217, 238).

das „wahre Recht" aufzufinden.[167] Am Ende des Auslegungsprozesses steht mithin ein normativ zwingendes Ergebnis.[168] Für das Unionsrecht ist diese Auslegungsmethodik freilich nicht hinreichend, denn vielmehr als lediglich um die Erreichung und Darstellung einer vertretbaren Entscheidung geht es darum, innerhalb eines vorliegenden Kontexts eine juristische Entscheidung nach bestimmten Regeln zu erzielen.[169] *Koch/Rüßmann* sprechen daher auch von der juristischen Methodenlehre als Begründungslehre.[170] In diesem Sinne handelt es sich bei den europarechtlichen Methodiken allerdings nicht um eine grundsätzliche Ablehnung der hermeneutischen Lehre. Stattdessen wird deren Systematisierungsleistung anerkannt und genutzt, jedoch auch deren Unfähigkeit zur umfassenden Interpretation von offenen Verfassungstexten erkannt und als Ansatzpunkt für weitergehende Auslegungsansätze erachtet.

Die vier bekannten Kanones bilden dementsprechend, leicht modifiziert gegenüber der klassischen Interpretation nationaler Gesetze, die Grundlage auch eines EU-rechtlichen Auslegungsvorgangs und werden um die rechtsvergleichende Auslegungsmethode erweitert.

aa. Grammatische Auslegung

Auch im Recht der Europäischen Union bildet die Wortlautauslegung den Ausgangspunkt der Begründung einer Entscheidung. Anders als bei der Auslegung deutschen Rechts kommt ihr jedoch keine „Grenzfunktion" zu. Dies zeigt sich beispielsweise an der Auslegung von Art. 288 AEUV durch den EuGH.[171] Dieser Unterschied zum nationalen Recht resultiert insbesondere aus der sprachlichen Diversität einer Vielzahl von gleichberechtigt nebeneinander stehenden Vertragstexten. Dadurch lässt sich nur schwerlich ein verbindlicher Wortlaut, der eine solche kategorische Grenze darstellen würde, finden. Folglich verwendet der EuGH die grammatische Auslegung lediglich als Ausgangspunkt für weitergehende Interpretationen oder abschließend zur Unterstützung eines bereits mit anderen Methoden gefundenen Ergebnisses.[172]

---

[167] Einen Überblick zur rechtlichen Hermeneutik der Neuzeit seit *von Savigny* bietet *Corzillius*, in: Böhl/Reinhard/Walter (Hrsg.), Hermeneutik, S. 308 ff.

[168] Vgl. *Müller/Christensen*, Juristische Methodik Bd. 2 – Europarecht, S. 28.

[169] *Nettesheim*, in: Oppermann/Classen/ders. (Hrsg.), Europarecht, § 9 Rn. 166.

[170] *Koch/Rüßmann*, Juristische Begründungslehre, S. 48 ff.

[171] *Nettesheim*, in: Oppermann/Classen/ders. (Hrsg.), Europarecht, § 9 Rn. 170, indem trotz eines sehr klaren Wortlauts teleologische Argumente bei der Zuerkennung der unmittelbaren Wirkung von Richtlinien angeführt werden.

[172] *Schroeder*, JuS 2004, 180 (182).

bb. Systematische Auslegung

Der systematischen Auslegung liegt das Gebot der Einheitlichkeit des Unionsrechts zugrunde.[173] Geprüft wird, ob sich ein Auslegungsergebnis mit anderen Bestimmungen des Unionsrechts vereinbaren lässt, oder sogar, ob jene Entscheidung anderen Bestimmungen besonders gerecht wird.[174] Daher zeigt sich in der Rechtsprechung des EuGH ein sog. dynamisch-evolutives Verständnis des Unionsrechts, wonach die Perspektive auf das geschriebene Recht durch politische, ökonomische und ökologische Veränderungen wandelbar ist.[175]

Die systematische Auslegungsmethodik hat sich in der Vergangenheit in der Regel integrationsbeschleunigend ausgewirkt. Spätestens mit dem Vertrag von Lissabon wurden aber dementgegen vermehrt ausdrücklich desintegrative Elemente ins europäische Primärrecht eingefügt. So wurde beispielsweise das Subsidiaritätsprinzip, das sich in ähnlicher Form bereits seit dem Maastrichter Vertrag im EU-Recht findet, in Art. 5 Abs. 3 EUV und die Identitätsklausel in Art. 4 Abs. 2 S. 1 EUV aufgenommen. Auch der strafrechtliche Notbremsemechanismus des Art. 83 Abs. 3 AEUV will einen stetig fortschreitenden und den Mitgliedstaaten entzogenen Integrationsprozess begrenzen.[176] Eine korrekte systematische Interpretation hat daher auch diesen integrationsbremsenden Aspekten Rechnung zu tragen.[177]

cc. Historische Auslegung

Einer historischen Auslegung unter Beachtung der Intentionen von Vertrags- oder Gesetzgeber im EU-Recht kommt nur eine sehr untergeordnete Rolle zu.[178] Einerseits ist die Erforschung des Willens der Normgeber mit Schwierigkeiten bei der Bestimmung der handelnden Personen und dem Umgang mit Uneinigkeiten im Rechtssetzungsprozess verbunden.[179] Andererseits bekennen sich die Organe der Europäischen Union ganz bewusst zu einer dynamischen Ordnung des EU-Gebildes, sodass die fraglichen Normen vor allem im Lichte der aktuel-

---

[173] EuGH, Rs. C-499/04, Slg. 2006, I-2397, Rn. 32 – *Werhof/Freeway Traffic Systems*.

[174] *Epiney*, in: Bieber/ders./Haag (Hrsg.), Europäische Union, § 9 Rn. 16.

[175] *Meyer*, in: von der Groeben/Schwarze/Hatje (Hrsg.), Vor Art. 82–86 AEUV Rn. 36.

[176] Einzelheiten zu diesen desintegrativen Elementen des Unionsrechts finden sich unten, Kap. 3 § 12 D II.

[177] Bereits seit dem Inkrafttreten des Vertrags von Maastricht erkennt *Shaw*, OJLS 1996, 231 (240 ff.), erste desintegrative Elemente im EU-Recht.

[178] Insoweit herrscht in der EU-rechtlichen Literatur weitgehende Einigkeit: *Buck*, Auslegungsmethoden, S. 151; *Kutscher*, EuR 1981, 392 (393); *Müller/Christensen*, Juristische Methodik Bd. 2 – Europarecht, S. 66; *Plender*, in: Yearbook of European Law, S. 57 (102 f.).

[179] *Epiney*, in: Bieber/ders./Haag (Hrsg.), Europäische Union, § 9 Rn. 15 .

len Integrationsziele zu lesen sind.[180] Eine am historischen Gehalt orientierte Normauslegung wäre daher ungenau und fehlerbehaftet sowie konträr zu den absichtlich veränderlichen Zielbestimmungen in der Politik der Europäischen Union. Überspitzt könnte man daher sogar sagen, dass die historische Auslegung bereits einer historischen Interpretation ablehnend gegenübersteht.

dd. Teleologische Auslegung

Teleologische Ansätze spielen bei der Auslegung des Unionsrechts eine besonders wichtige Rolle. Die teleologische Auslegung orientiert sich dabei am normativ gesetzten Zielzustand des EU-Rechts.[181] Die Hervorhebung dieser Auslegungsmethode hat es dem EuGH mehrfach ermöglicht, integrationsrechtliche Quantensprünge herbeizuführen, wofür seine Rechtsprechung zur Absicherung der einheitlichen und gleichen Wirksamkeit des EU-Rechts in allen Mitgliedstaaten exemplarisch steht.[182] Der EuGH hat etwa in der sog. Becker-Rechtsprechung festgestellt, dass die praktische Wirksamkeit von Richtlinien gegenüber den Mitgliedstaaten dann am höchsten ist, wenn diese unmittelbare Wirkung entfalten.[183] In seiner sog. Francovich-Rechtsprechung bemerkte der Gerichtshof, dass die „volle Wirksamkeit" des EU-Rechts erst durch einen Staatshaftungsanspruch bei Verletzung desselben garantiert ist.[184] Entgegen der traditionellen Hierarchie der Auslegungsmethoden steht die teleologische Methode im europäischen Recht, ihrer Gewichtung entsprechend, am Anfang der Auslegung und die Wortlautauslegung am Ende.[185]

Dementsprechend ist Auslegung nach Sinn und Zweck der primärrechtlichen Norm wesentliches Element nahezu sämtlicher Entscheidungen des EuGH. Obwohl oftmals angeführt wird, dass sich die dynamisch-teleologische Auslegung am „Geist der Verträge", am „Zweck des Gesetzes" oder an einen „objektivierten Willen" orientiere,[186] führt ein solches Verständnis der dynamisch-teleologischen Methodik letztlich wieder zum bereits angesprochenen Ausgangspunkt,

---

[180] Vgl. *Pechstein/Drechsler*, in: Riesenhuber (Hrsg.), Europäische Methodenlehre, § 7 Rn. 33.

[181] Vgl. u. a. *Hahn-Lorber*, ECJ 2010, 760 (764 f.).

[182] *Nettesheim*, in: Oppermann/Classen/ders. (Hrsg.), Europarecht, § 9 Rn. 176 und *ders.*, in: GS-Grabitz (1995), S. 447 (463 ff.).

[183] EuGH, Rs. 8/81, Slg. 1982, 53, Rn. 23 ff. – *Becker*.

[184] EuGH, verb. Rs. C-6/90 und C-9/90, Slg. 1991, I-5359, Rn. 33 – *Francovich*.

[185] Gleichwohl weist *Meyer*, Strafrechtsgenese, S. 343, unter Bezugnahme auf EuGH, Rs. 26/62, Slg. 1963, 3 (24) – *van Gend & Loos*, darauf hin, dass der teleologische Ansatz bei der Auslegung durchaus eine gewisse Dominanz aufweist.

[186] *Schroeder*, JuS 2004, 180 (183); kritisch zu dieser Sichtweise *Nettesheim*, in: Oppermann/Classen/ders. (Hrsg.), Europarecht, § 9 Rn. 177.

dass ein quasi „im Verborgenen" liegendes richtiges Ergebnis durch Interpretation erreicht werden müsse. Insbesondere im EU-Recht ist ein solches Verständnis allerdings wenig zielführend, da sich in den Verträgen eine Vielzahl von Anhaltspunkten findet, die eine denkbar große Bandbreite an „richtigen" Auslegungsergebnissen zulässt.[187]

Aufrichtiger und transparenter erscheint hingegen die Erkenntnis, dass eine klassisch-hermeneutische Betrachtung der Vertragstexte keine ausreichende Grundlage zur Auslegung bilden kann. Das Eingeständnis der begrenzten Tauglichkeit des klassischen juristischen Auslegungskanons ist somit ein Beitrag zur Methodenehrlichkeit.[188] Selbst Vertreter klassischer Auslegungsvorgänge scheinen das im Grunde zu akzeptieren, verschleiern dieses Eingeständnis jedoch regelmäßig durch die extensive Ausreizung systematischer und teleologischer Argumentationsstränge. Dadurch kommt es oftmals zur Überfrachtung der Auslegung anhand von Sinn und Zweck, die einer echten dynamisch-teleologischen Interpretation nicht mehr gerecht wird. Im EU-Recht wird allerdings nicht lediglich durch Wortlaut, Systematik, Historie und Teleologie ein „richtiges" Auslegungsergebnis angestrebt. Der Begründungsprozess mit seinen vielfältigen Methoden zielt vielmehr auf ein im Gesamtkonzept des EU-Rechts verankertes Interpretationsziel ab.

Wie einerseits das vor allem in der nationalen Rechtswissenschaft anzutreffende[189] Verständnis, der EuGH nutze und sprenge die klassischen Auslegungskanones durch eine Überbetonung systematischer und teleologischer Erwägungen, und andererseits eine im Mehrebenensystem notwendige Verknüpfung mitgliedstaatlicher und EU-rechtlicher Interpretationsprinzipien in Einklang zu bringen sind, wird im Folgenden noch zu evaluieren sein.

Die Emanzipation der Verfassungsinterpretation von der einfachen Gesetzesauslegung,[190] die umso dringender auch auf EU-Ebene angebracht ist, zeigt sich insbesondere durch die Hinzuziehung der rechtsvergleichenden Auslegungsmethodik, weiterer Methoden sowie der Konsultation außerrechtlicher Aspekte im Interpretationsvorgang. Nur ein Verständnis jener Elemente ergibt ein vollständiges Bild des Interpretationsvorgangs im Recht der EU.

---

[187] Vgl. *Nettesheim*, in: Oppermann/Classen/ders., Europarecht, § 9 Rn. 177.

[188] Obwohl das EU-Recht selbstverständlich auch nationalstaatliche Auslegungstraditionen achtet und deren Methoden verwendet, werden diese teilweise eigenständig interpretiert und vor allem durch zusätzliche methodische Elemente ergänzt; dazu auch *Müller/Christensen*, Juristische Methodik Bd. 2 – Europarecht, S. 27.

[189] Siehe beispielhaft die Ausführungen bei *Pechstein/Drechsler*, in: Riesenhuber (Hrsg.), Europäische Methodenlehre, § 7 Rn. 40.

[190] *Böckenförde*, NJW 1976, 2089; *Häberle/Kotzur*, Europäische Verfassungslehre, S. 486.

ee. Rechtsvergleichende Auslegung

Die rechtsvergleichende Auslegungsmethode ist im Primärrecht in Art. 6 Abs. 3 EUV verankert, der die gemeinsamen Verfassungsüberlieferungen der Mitgliedstaaten als heranzuziehende Rechtsquellen des Unionsrechts anerkennt.[191] Teilweise wird die Rechtsvergleichung gar als „fünfte Auslegungsmethode“ des EU-Rechts bezeichnet.[192] Dabei spielt sie als „wertende Rechtsvergleichung“, die sich letztlich nur den zweckmäßigsten der verglichenen Rechtsvorschriften bedient,[193] zwar eine wichtige Rolle bei der Auslegung von europäischem Primärrecht, ist aber doch als Hilfsmethodik einzuordnen. So nutzt der EuGH die rechtsvergleichende Auslegung in der Regel zur Lückenfüllung anhand allgemeiner Rechtsgrundsätze, da die Verträge nicht zwingend das in der Europäischen Union geltende Recht widerspiegelten und daher eine Konkretisierung möglich und geboten sei.[194]

ff. Bedeutung für den Auslegungsprozess

Die „wertende Rechtsvergleichung“ und die Sonderstellung der Auslegung anhand des Grundsatzes der Zweckmäßigkeit lassen die Auslegung im Unionsrecht von dem Ziel einer möglichst exakten Ermittlung des Norminhalts in die Grauzone zur Rechtsfortbildung übertreten. Dabei ist anzuerkennen, dass die Europäischen Verträgen als sog. offene Verfassungstexte es erfordern, dass die Auslegungsorgane Konkretisierung, Lückenfüllung und Rechtsfortbildung betreiben, um vielen Aspekten überhaupt erst einen sinnstiftenden Inhalt zu geben. So erkennt auch etwa die französische Methodenlehre diese Vermengung der Auslegung unbestimmter Rechtsbegriffe, Schließung von Regelungslücken und einer Neuschöpfung von Recht durch die EuGH-Rechtsprechung als zulässigen Teil des Auslegungsvorgangs („interprétation“) an.[195]

Neben der bereits angesprochenen Herausforderung der Mehrsprachigkeit des EU-Rechts und der damit einhergehenden Abwertung einer grammatischen

---

[191] *Müller/Christensen*, Juristische Methodik, Bd. 2 – Europarecht, S. 118; siehe auch *Schroeder*, JuS 2004, 180 (184), der sich freilich noch auf Art. 6 Abs. 2 EUV a. F. bezieht; *Pernice*, in: Schulze-Fielitz (Hrsg.), Staatsrechtslehre als Wissenschaft, S. 225 (244 f.), macht darüber hinaus deutlich, dass die Rechtsvergleichung im klassischen Sinne zwar für einzelne Auslegungsfragen hinreichend sein könne, die Entwicklung einer wirklichen europäischen Rechtswissenschaft mit eigenständiger Auslegungsmethodik jedoch vielmehr einen horizontalen Dialog erfordere.

[192] So *Häberle*, JZ 1989, 913 (916 f.).

[193] *Schroeder*, JuS 2004, 180 (184).

[194] Siehe insb. *Häberle/Kotzur*, Europäische Verfassungslehre, S. 504 f.; *Schroeder*, JuS 2004, 180 (183) m. w. N.

[195] *Schroeder*, JuS 2004, 180 (184) m. w. N.

Auslegungsmethode spielt auch die Begriffsautonomie des europäischen Rechts eine wesentliche Rolle. Nur so kann die Eigenständigkeit der Unionsrechtsordnung gegenüber dem mitgliedstaatlichen Recht bestehen und die Verwirklichung von EU-Zielen sichergestellt werden. Nationalstaatliche Auslegungsansätze könnten stattdessen zu einer Umgehung oder Aufweichung der Unionsrechtsordnung führen. Das EU-Recht ist von seiner Grundkonzeption her steuerungsgetrieben,[196] also politisch aufgeladen. Die Vorschriften sind regelmäßig zielgeleitet ausgestaltet, was sich insbesondere im Grundsatz des *effet utile* zeigt, der auf die „volle Wirksamkeit" des EU-Rechts ausgerichtet ist.[197]

Dennoch ist der oft vertretenen oberflächlichen Sichtweise, das EU-Recht fange beim klassisch-hermeneutischen Interpretationsvorgang auftretende Lücken lediglich durch die Akzentuierung des dynamisch-teleologischen Ansatzes auf, entgegenzutreten. Auch wenn der EuGH in der Vergangenheit oftmals als „Motor der Integration" wahrgenommen worden ist, da er Unklarheiten vielfach zugunsten des Unionsrechts aufgelöst hat, fußt dies weniger auf einer Überreizung der systematischen und teleologischen Methoden. Vielmehr resultiert dies aus der Anwendung eines deutlich vielfältigeren Interpretationsgefüges. Im Folgenden werden daher methodische Erweiterungen zu den klassischen juristischen Auslegungsmethoden erläutert, um den europäischen Auslegungsvorgang im Primärrecht umfassender abbilden zu können. Gerade für das Strafrecht als eine vor Lissabon nahezu als integrationsfest empfundene Materie lassen sich im EU-Primärrecht desintegrative Elemente erkennen, die eine reine *effet-utile*-Betrachtung weder rechtmäßig noch überwiegend wahrscheinlich erscheinen lassen.

b. Methodische Erweiterungen

Um den Auslegungsvorgang des EuGH bezüglich Kompetenznormen nachvollziehen und daraufhin dessen Auslegungsergebnis für den Begriff der Computerkriminalität in Art. 83 Abs. 1 UAbs. 2 AEUV mitgestalten zu können, sind die weiteren Auslegungsmethoden des EuGH zu berücksichtigen. Dabei handelt es sich insbesondere um die *topisch-problemorientierte* Interpretation,[198] die Beachtung und Verwertung außerrechtlicher Aspekte bei der Entscheidungsfindung[199] sowie die Einbeziehung der Entscheidungen anderer europäischer (Ver-

---

[196] Vgl. *Pechstein/Drechsler*, in: Riesenhuber (Hrsg.), Europäische Methodenlehre, § 7 Rn. 11.

[197] Vgl. *Schroeder*, JuS 2004, 180 (185 ff.).

[198] Siehe unten, Kap. 2 § 7 C. I. 2. b. aa.

[199] Siehe unten, Kap. 2 § 7 C. I. 2. b. bb.

fassungs-)Gerichte in seinen Auslegungsprozess im Rahmen eines Verfassungsgerichtsdialogs[200].

aa. Weitere Methoden der europäischen Verfassungsinterpretation

Wie bereits angedeutet, herrscht weitestgehend Einigkeit darüber, dass Verfassungen als offen gestaltete Grundlagentexte nicht ausschließlich durch die klassisch-hermeneutischen Methoden der Gesetzesauslegung interpretiert werden können.[201] Verfassungen können nur fragmentarischen Charakter aufweisen und lediglich eine ausfüllungsbedürftige Grundlage mit groben Regelungsstrukturen für die rechtlichen Aspekte des gesellschaftlichen Zusammenlebens bieten.

Auf Ebene der Europäischen Union kommt erschwerend hinzu, dass das Europäische Verfassungsrecht kein in sich geschlossener und stringent entwickelter Normkörper ist, dem eine grundsätzlich zeitlose Komponente innewohnt, wie es bei den meisten nationalstaatlichen Verfassungen der Fall ist. Vielmehr ist das Europäische Verfassungsrecht „durch die in sich verschraubten Rechtstraditionen, Regelungsebenen und institutionellen Entwicklungen“[202] einer inhärenten Offenheit ausgesetzt. Diese ist nicht zuletzt auch darauf gegründet, dass neu aufzunehmende Mitglieder ihre nationalen Rechtstraditionen nicht beim „Einzug nach Brüssel“ abgeben müssen. Vielmehr stellen diese Traditionen von jenem Zeitpunkt an gem. Art. 6 Abs. 3 EUV einen relevanten Auslegungsaspekt im europäischen Interpretationsprozess dar. Zusätzlich zu diesen mitgliedstaatlichen Rechtsgrundsätzen und -traditionen erweitern mehrere Ansätze zur (europäischen) Verfassungsinterpretation das Gesamtbild und bieten dadurch erst die Möglichkeit, den europäischen Auslegungsprozess nachvollziehen und ihn nicht wie eine Aus- oder sogar Überdehnung der dynamisch-teleologischen Auslegungsmethodik begreifen zu können.

Die sog. topisch-problemorientierte Methodik setzt im Rahmen der Verfassungsinterpretation an der Leerstelle an, die nach Anwendung der klassischen Hermeneutik verbleiben kann. Sie hat insbesondere das Ziel, trotz eines strukturell offenen und fragmentarischen Verfassungstexts ein *non liquet* zu vermeiden. Dabei wird nicht der Norminhalt und das juristische System in den Vordergrund gestellt, sondern dem Problem das Primat im Auslegungsprozess zugesprochen.[203] Nicht die Ermittlung des „wahren“ Norminhalts durch die

---

[200] Siehe unten, Kap. 2 § 7 C. I. 2. b. cc.

[201] *Häberle/Kotzur*, Europäische Verfassungslehre, S. 54 ff.; a. A. damals noch *Larenz*, Methodenlehre, S. 148.

[202] *Haltern*, in: Schuppert/Pernice/ders. (Hrsg.), Europawissenschaft, S. 37 (47).

[203] *Böckenförde*, NJW 1976, 2089 (2092); *Häberle*, JZ 1989, 913 (916), spricht insoweit

konsequente Befolgung von Auslegungsregeln stellt die Interpretationsmethodik dar, vielmehr werden die von einer Verfassung geschützten Rechtsgüter und deren Leitprinzipien als Bausteine[204] aufgefasst, die je nach Fall- bzw. Problemkonstellation zur Interpretation herangezogen werden.[205] Auch in der Rechtsprechung des Bundesverfassungsgerichts ist die *topisch-problemorientierte* Verfassungsinterpretation oftmals anzutreffen, wobei häufig kritisch angemerkt wird, dass diese Interpretationsmethodik weniger eine Inhalts*ermittlung*, als vielmehr eine Inhalts*bestimmung* bezeichne.[206] Diese politische Beeinflussung des Auslegungsvorgangs könne nur dann einer Beliebigkeit entgehen, wenn Konsens sowohl bezüglich des Bestands als auch des Inhalts der Verfassung bestünde.[207] Dies kann das EU-Primärrecht als zumindest verfassungsähnlicher Rechtstext jedoch nicht aufweisen, da man weder von einem allgemein akzeptierten Bestand noch einem unstreitigen Inhalt sprechen kann. Oftmals wird demnach rückwärts argumentiert, indem versucht wird, eine tatsächliche Problemstellung mit dem EU-Recht zu lösen. Daran zeigt sich der Unterschied zwischen einem „ergebnissuchenden" und einem „ergebnisbegründenden" Interpretationsprozess.

Noch weiter geht die sog. wirklichkeitswissenschaftlich orientierte Verfassungsinterpretation, die auf die Integrationslehre *Smends* zurückgeht.[208] Auch diese Methode zielt auf die Verhinderung von ergebnislosen Auslegungsvorgängen anhand der klassisch-juristischen Hermeneutik ab. Sie legt den Verfassungstext dazu nach dessen Sinn und Wirklichkeit und nicht anhand des Wortlauts und der dogmatischen Begrifflichkeiten aus.[209] Auf der Basis dieser Betrachtungsweise findet eine grundlegende Änderung im Auslegungsprozess statt. So werden nicht mehr normative Größen, wie die Prinzipien und Grundentscheidungen des Verfassungsgebers, sondern aktuelle Wirklichkeitsbeobachtungen und etwaige soziale Funktionen einer Verfassung herangezogen.[210] Gerade im Rahmen einer politisch motivierten sowie durch gemeinsame politi-

---

auch vom „Postulat von der gerechtigkeits- bzw. vernunftsorientierten Ergebniskontrolle" und macht deutlich, dass jeder erfahrene Richter vom Ergebnis her denke, was jedoch durch seine Schulung in den klassischen Auslegungsmethoden letztlich unproblematisch sei.

[204] *Ehmke*, VVDStRL 1963 Bd. 20, S. 53 (62 f.), prägt in diesem Zusammenhang den Begriff des „Verfassungsrechtsmaterials".

[205] *Böckenförde*, NJW 1976, 2089 (2092) m. w. N.

[206] *Böckenförde*, NJW 1976, 2089 (2092 f.).

[207] *Böckenförde*, NJW 1976, 2089 (2094).

[208] *Smend*, Verfassung und Verfassungsrecht, S. 75 ff.

[209] *Böckenförde*, NJW 1976, 2089 (2094) m. w. N.

[210] *Böckenförde*, NJW 1976, 2089 (2095), bezugnehmend auf *Richter*, Bildungsverfassungsrecht, S. 26 f.

sche und wirtschaftliche Ziele definierten Europäischen Union findet dieser interpretatorische Ansatz Gehör.

bb. „Recht &"-Methoden

Auf diesen Methoden aufbauend stellt etwa *Häberle* über die Methodik der Verfassungsinterpretation hinaus gar den Kreis der am Interpretationsprozess Beteiligten zur Disposition und spricht dem Auslegungsvorgang die staatliche und dadurch auch die verfassungsgerichtliche Exklusivität ab. Vielmehr seien auch die demokratische und pluralistische Öffentlichkeit, die Medien und die Politik am Auslegungsprozess beteiligt.[211] Etwas weniger radikal bezüglich der Teilhabe verschiedener Akteure am verfassungsrechtlichen Auslegungsvorgang und vor allem auf die Besonderheiten des EU-Rechts bezogen, versucht *Haltern*, kulturwissenschaftliche Elemente zu etablieren und entwirft daher die Figur des „Rechts im Kontext". Insbesondere die Europäische Union beschäftige ein Grundrechts-, Werte-, und Verfassungsdiskurs, der viel Material zur Verfügung stelle, um einen theoretischen Anschluss an die Politik-, Sozial-, und Wirtschaftswissenschaften zu suchen.[212] *Hahn-Lorber* spricht insoweit von einem „inclusive reasoning", um auf die Empfänglichkeit eines offenen, sich dynamisch entwickelnden Verfassungstexts aufmerksam zu machen.[213] Seiner Ansicht nach handelt es sich vor allem beim europäischen Primärrecht um Meta-Normen, die keinesfalls ausschließlich innerrechtlich ausgelegt werden dürften, sondern jeweils an die politischen und sozialen Grundlagen des Verfassungstexts rückzukoppeln seien.[214]

Die interpretatorischen Ansätze von „Recht &"-Methoden zielen vor allem auf eine Verschränkung der Rechtswissenschaft mit anderen Geisteswissenschaften, um der prinzipiellen reinen Innenperspektive der Rechtswissenschaft zusätzliches Auslegungsmaterial zur Verfügung zu stellen. Die aktuelle Konstruktion der Europäischen Union mit vielen staatsanalogen Elementen einerseits und zahlreichen hinter einem modernen demokratischen Staatsverständnis zurückbleibenden Aspekten[215] andererseits erscheint besonders dazu geeignet, außerrechtlichen Auslegungskriterien einen entsprechenden Raum zu bieten. Die Verschränkung von drei Ebenen (Bürger, Nationalstaat und Union) mit wechselnder Festlegung von Horizontal- oder Vertikalverhältnissen untereinan-

---

211 *Häberle/Kotzur*, Europäische Verfassungslehre, S. 496 ff.
212 *Haltern*, in: Schuppert/Pernice/ders. (Hrsg.), Europawissenschaft, S. 37 (81 f.).
213 *Hahn-Lorber*, ELJ 2010, 760 (765).
214 *Hahn-Lorber*, ELJ 2010, 760 (761).
215 Als Beispiel sei hier die fehlende Rückkoppelung der europäischen Legislative an einen gesamt-europäischen Souverän genannt.

der ist noch mehr als ein nationalstaatliches Gefüge mit lediglich zwei Ebenen dazu prädestiniert, etwa politik- oder wirtschaftswissenschaftliche Argumente auch in rechtliche Auslegungsvorgänge einzubeziehen. Dafür spricht zudem der Umstand, dass es sich bei der EU geschichtlich um ein wirtschaftliches Integrationsprojekt handelt, dessen Verwirklichung oftmals politische Entscheidungen erfordert. Dem so verstandenen Unionsrecht können starre juristische Auslegungskriterien nicht gerecht werden.

cc. Dialog im Europäischen Verfassungsgerichtsverbund

Weniger eine echte Methodik, wohl aber eine Grundbedingung für den konstitutionellen Zusammenhalt der Europäischen Union und unabdingbar für ein Verständnis der Auslegung des EuGH ist der sog. Dialog im Europäischen Verfassungsgerichtsverbund. Dieser von *Voßkuhle*[216] geprägte Begriff enthält zwei besonders relevante Aspekte, die den Auslegungsprozess zum europäischen (Primär-)Recht beeinflussen.

Erstens geht *Voßkuhle* davon aus, dass neben den nationalen Verfassungsgerichten[217] auch der EuGH und der EGMR jeweils als (europäische) Verfassungsgerichte einzuordnen seien.[218] Dabei weist er auf die Vorarbeiten zur Wandlung der Stellung des Bundesverfassungsgerichts durch den Bedeutungszuwachs der europäischen Gerichte[219] sowie auf neuere Arbeiten zum Begriff der Europäischen Verfassungsgerichte[220] hin und baut auf diesen auf. Zweitens zeigt er auf, dass eine Letztendscheidungskompetenz weder dem EuGH noch dem Bundesverfassungsgericht zukommt. Darüberhinaus legt er dar, weshalb den Verlaut-

---

[216] Laut *Brunkhorst*, in: Albert/Stichweh (Hrsg.), Weltstaat und Weltstaatlichkeit, S. 63 (77) geht der Begriff eigentlich auf *di Fabio*, Der Verfassungsstaat in der Weltgesellschaft, S. 78, zurück. Dieser spricht allerdings von der „Kooperation der Verfassungsgerichte im überstaatlichen Verbund“, wie *Voßkuhle* selbst anmerkt; vgl. insoweit *Voßkuhle*, NVwZ 2010, 1 (3).

[217] *Voßkuhle* beschränkt sich hier im Wesentlichen zwar auf die Zusammenhänge zwischen dem BVerfG und dem EuGH bzw. dem EGMR, grundsätzlich sind seine Ausführungen aber auch auf die anderen nationalen Verfassungsgerichte der EU-Mitgliedstaaten übertragbar; vgl. dazu *Voßkuhle*, NVwZ 2010, 1 (10); ähnlich aus Sicht des EuGH auch *Lenaerts/Gutiérrez-Fons*, EUI Working Paper AEL 2013/09, 3 (48).

[218] *Voßkuhle*, NVwZ 2010, 1 (2 f.); obwohl *Voßkuhle* das Verbundsystem sowohl hinsichtlich des EuGH als auch des EGMR untersucht, konzentriert sich dieser Abschnitt naheliegenderweise auf den Verbundgedanken zwischen BVerfG und EuGH.

[219] *Hesse*, JZ 1995, 265 (269).

[220] *Häberle/Kotzur*, Europäische Verfassungslehre, S. 778 ff.; *Iglesias*, in: Walter-Hallstein-Institut für Europa (Hrsg.), Europäische Verfassung in der Krise, S. 107 (110 f.); *Mayer*, in: von Bogdandy/Bast (Hrsg.), Europäisches Verfassungsrecht, S. 559 (560 ff.).

barungen eines jeweiligen Verfassungsgerichts gleichwohl ein maßgeblicher Anteil am Auslegungsprozess des jeweils anderen zusteht.

Der Verbundgedanke nimmt dabei eine Art Klammerfunktion für diese beiden Aspekte ein. Zunächst drückt die Einordnung des EuGH als Verfassungsgericht gemeinsam mit dem Verbundbegriff die fehlende Festlegung einer Hierarchie zwischen den verschiedenen Gerichten aus, indem auf wertende Begriffe der Gleich-, Unter- oder Überordnung verzichtet wird.[221] Zusätzlich ist er an die europäischen Begriffe des „Staatenverbunds" aus dem Maastricht-[222] und dem Lissabon-Urteil[223] des Bundesverfassungsgerichts und des „europäischen Verfassungsverbundes" angelehnt, der u. a. durch *Pernice*[224] und *Calliess*[225] geprägt worden ist. Damit wird auf ein grundsätzlich bekanntes und anerkanntes Ordnungskonzept zurückgegriffen.

Daneben, und an dieser Stelle von besonderer Relevanz, kommt durch den Begriff eines Verfassungsgerichtsverbundes der gemeinsame Anteil an europäischen Auslegungsprozessen zum Ausdruck. Zwar ist die Aufgabenverteilung zwischen BVerfG und EuGH grundsätzlich eindeutig. Das BVerfG begleitet den Integrationsprozess der Europäischen Union von national-verfassungsrechtlicher Warte, während der EuGH rechtliche Prüfungen ausschließlich anhand des Unionsrechts vornimmt. Jedoch sind die Abgrenzungen von Kompetenzen zwischen den Gerichten in einem komplexen Mehrebenensystem wie der Europäischen Union trotz dieser vermeintlich eindeutigen Ausgangslage nicht immer zweifelsfrei möglich.[226] Umso wertvoller ist daher die Absage *Voßkuhles* an den Wurf eines „Fehdehandschuhs"[227] und eine „Karlsruher Totalaufsicht"[228], wie das Verhältnis zwischen EuGH und Bundesverfassungsgericht in der deutschen rechtswissenschaftlichen Litertaur bisweilen charakterisiert wird. Vielmehr bekräftigt er ausdrücklich den Vorrang des Gemeinschaftsrechts gegenüber mit-

---

[221] *Voßkuhle*, NVwZ 2010, 1 (3).

[222] BVerfGE 89, 155 (188 ff.).

[223] BVerfGE 123, 267 (348).

[224] *Pernice*, JöR n. F. 48 (1999), S. 205 ff.; *ders.*, Verfassungsverbund, S. 17 ff.; *ders.*, in: Calliess (Hrsg.), Verfassungswandel im europäischen Staaten- und Verfassungsverbund, S. 61 ff.; *ders.*, CJEL 15 (2009), 349 ff.

[225] *Calliess*, in: ders./Ruffert (Hrsg.), Art. 1 EUV Rn. 33 ff.

[226] Insb. *Pernice*, ZaöRV 70 (2010), 51 (62 ff.), verdeutlicht, dass dem Gedanken eines Verbundssystems inhärent ist, dass keine klare Hierarchisierung zwischen den horizontal vernetzten Akteuren herzustellen ist.

[227] *Oppermann*, EuZW 2009, 473.

[228] *Calliess*, Unter Karlsruher Totalaufsicht, FAZ v. 27.8.2009; abrufbar unter: http://www.faz.net/aktuell/politik/staat-und-recht/gastbeitrag-unter-karlsruher-totalaufsicht-1845469.html (Stand: 21.3.2017).

gliedstaatlichem (Verfassungs-)Recht,[229] betont dabei allerdings, dass dieser Vorrang nicht genuin aus dem EU-Recht fließe, sondern auf verfassungsrechtliche Entscheidungen der Mitgliedstaaten zurückgehe und daher grundsätzlich auch durch jene begrenzt und begrenzbar sei.[230]

Dieses Verständnis eines Europäischen Verfassungsgerichtsverbunds schafft die Notwendigkeit eines Dialogs der Verfassungsgerichte im europäischen Mehrebenensystem. Es bietet damit eine Art Sollbruchstelle, an welcher die Erwägungen der nationalen Verfassungsgerichte in den Auslegungsvorgang des EuGH einfließen können. Obwohl der EuGH selbstständig und final über die Auslegung des EU-Rechts entscheidet, und damit „Herr des europäischen Auslegungsvorgangs" ist, finden die Verlautbarungen der mitgliedstaatlichen Verfassungsgerichte bei seinen Entscheidungen und, häufig noch sichtbarer, bei politischen Entscheidungen der weiteren EU-Institutionen Beachtung. Für die Vergangenheit bietet die bekannte Solange-Rechtsprechung des Bundesverfassungsgericht hinsichtlich eines ausreichenden Grundrechtsschutzes[231] ein Beispiel für einen gelungenen Dialog zwischen Bundesverfassungsgericht und dem EuGH. Die Europäische Union hat die Kritik des Bundesverfassungsgericht aus dem ersten Solange-Urteil konstruktiv aufgenommen und den Grundrechtsschutz im Geltungsbereich des Gemeinschaftsrechts kontinuierlich ausgebaut.[232] Daraufhin hat das Bundesverfassungsgericht in der Solange-II-Entscheidung seinen Grundrechtsschutz auf EU-Ebene zurückgenommen. Aktuelle Instrumente der Teilhabe am Integrations- und Interpretationsprozess des EuGH durch die nationalen Verfassungsgerichte bieten die durch das Bundesverfassungsgericht und andere europäische Verfassungsgerichte entwickelten *Ultra-vires*- und Identitätskontrollen.[233] *Voßkuhle* merkt darüber hinaus an, dass die aktuelle Rechtsprechung des EuGH durchaus Tendenzen zu restriktiven Momenten erkennen lasse und die Besorgnis einer extensiven Nutzung erweiternder Auslegungsmethoden zurzeit unbegründet erscheint.[234] Auch wenn eine Kausalität schwerlich nachzuweisen ist, liegt die Vermutung nahe, dass die

---

[229] *Voßkuhle*, NVwZ 2010, 1 (5 f.), unter Verweis auf BVerfGE 123, 267 (396 f.).

[230] In der Bundesrepublik Deutschland stelle etwa das jeweilige Zustimmungsgesetz zur Grundgesetzänderung eine derartige Brückenfunktion dar; vgl. dazu *Voßkuhle*, NVwZ 2010, 1 (6).

[231] BVerfGE 37, 271 ff.; BVerfGE 73, 339 ff.

[232] *Voßkuhle*, NVwZ 2010, 1 (6).

[233] Siehe bereits oben, Kap. 2 § 7 C. I. 1. b.

[234] *Voßkuhle*, NVwZ 2010, 1 (7), wobei er beispielhaft die Anerkennung von mitgliedstaatlichen Beschränkungen der Grundfreiheiten durch den vorrangigen Schutz der Menschenwürde (EuGH, Rs. C-36/02, Slg. 2004, I-9609 – *Laserdrome*), die Belange der Versammlungs- und Meinungsfreiheit (EuGH, Rs. C-112/00, Slg. 2003, I-5659 – *Brennerblockade*), den Schutz der nationalen Kultur (EuGH, Rs. C-260/89, Slg. 1991, I-2925 – *ERT/DEP*)

geäußerten verfassungsrechtlichen Bedenken der mitgliedstaatlichen (Verfassungs-)Gerichte den EuGH zu einer vorsichtigeren und dialogbereiten Rolle im Integrationsprozess anhalten.

Obgleich sowohl die faktischen Ausprägungen eines solchen Dialogs als auch seine Implikationen für die Methodik der jeweiligen Verfassungs- bzw. Primärrechtsauslegung bislang nicht als gesichert gelten können, ist die Existenz eines Kooperationsverhältnisses kaum zu leugnen. Daraus könnte sich zukünftig durchaus ein theoretisch-methodischer Überbau entwickeln.[235] Wie im weiteren Verlauf dieser Arbeit zu zeigen sein wird, sind auch im Bereich der Computerkriminalität Tendenzen zu erkennen, dass die bundesverfassungsgerichtliche Rechtsprechung beim Erlass von Harmonisierungsmaßnahmen beachtet wird. Daher kann und muss der Verfassungsgerichtsdialog, wenn auch (noch) nicht als klassisches methodisches, so doch zumindest als tatsächliches Element im europäischen Auslegungsprozess aufgefasst werden.

Damit wird auch deutlich, dass bei der Auslegung des europäischen Primärrechts die Entscheidungen des Bundesverfassungsgericht zwar keine unmittelbare Wirkung haben, ihre Beachtung durch den EuGH aber nicht nur auf einer „Drohkulisse" beruht, sondern quasi methodisch verankert ist und einen Teilaspekt des Dialogs im Europäischen Verfassungsgerichtsverbund darstellt.

II. Exkurs: Das Bundesverfassungsgericht und die Auslegung strafrechtlicher EU-Kompetenznormen

Nach der Unterzeichnung des Vertrags von Lissabon im Dezember 2007 durch die Staats- und Regierungschefs der Mitgliedstaaten der Europäischen Union war das Inkrafttreten noch von der Ratifizierung durch sämtliche EU-Mitgliedstaaten abhängig. In Deutschland haben dazu Bundestag und Bundesrat ein Zustimmungsgesetz nach Art. 23 Abs. 1 S. 2 GG erlassen,[236] das von einem Gesetz zur Änderung des Grundgesetzes[237] und von einem Begleitgesetz[238] flankiert wurde. Da jedoch mehrere Verfassungsbeschwerden gegen diese Gesetzgebung

---

oder die Bekämpfung der Kriminalität im Glücksspielsektor (EuGH, Rs. C-42/07, Slg. 2009, I-07633 – *Liga Portuguesa de Futebol Profissional*) anführt.

[235] *Ruggeri, A.,* in: Ruggeri, S. (Hrsg.), Human Rights in European Criminal Law, S. 10 (11).

[236] Das Zustimmungsgesetz der Bundesrepublik Deutschland zum Vertrag von Lissabon v. 13.12.2007 zur Änderung des Vertrags über die Europäische Union und des Vertrags zur Gründung der Europäischen Gemeinschaft (ABl. C 306 v. 17.12.2007, S. 1) hat der Deutsche Bundestag am 24.4.2008 verabschiedet, woraufhin der Bundesrat am 23.5.2008 zustimmte.

[237] BT-Drs. 16/8488.

[238] BT-Drs. 16/8489.

erhoben wurden,[239] wartete der damalige Bundespräsident Köhler mit der Unterzeichnung der Gesetze ab, bis sich das Bundesverfassungsgericht dazu geäußert hatte. Dieses fällte am 30. Juni 2009 sein vielbeachtetes „Lissabon-Urteil", das vor allem auch für das deutsche und europäische Strafrecht von besonderer Bedeutung gewesen ist.

1. Vereinbarkeit des Lissabon-Vertrags mit deutschem Verfassungsrecht

Die Beschwerdeführer stützten sich auf ihr Wahlrecht aus Art. 38 Abs. 1 GG und rügten einen Verlust der Staatlichkeit der Bundesrepublik Deutschland sowie eine mangelnde demokratische Legitimation der Europäischen Union. Die Verletzung des grundrechtsgleichen Wahlrechts aus Art. 38 Abs. 1 GG rühre daher, dass es durch signifikante Weichenstellungen in Brüssel faktisch seines Inhalts beraubt würde, ohne dass diese Kompetenzen durch eine adäquate demokratische Legitimation der Union aufgewogen würden. Das Bundesverfassungsgericht stimmt diesem Vorbringen der Beschwerdeführer im Ergebnis nicht zu.

Erstens hält das Bundesverfassungsgericht weiterhin daran fest, dass es sich bei der Europäischen Union um einen Staatenverbund und nicht um eine staatsanaloge Organisationsstruktur handele.[240] Damit bleibt es seiner Linie aus dem Maastricht-Urteil treu.[241] Einerseits seien die demokratischen Anforderungen an einen Bundesstaat nicht erfüllt, da es weder zu einem demokratischen Wettstreit[242] zwischen Regierung und Opposition komme, noch die Erfolgschancengleichheit[243] der Stimmen zum Europäischen Parlament gegeben sei. Andererseits komme im Vertrag von Lissabon auch kein Wille zur (Bundes-)Staatlichkeit der Europäischen Union zum Ausdruck, sodass vor diesem Hintergrund die demokratische Legitimation derzeitig als ausreichend zu erachten sei.[244]

Zweitens liege auch nach dem Vertrag von Lissabon kein untragbarer Souveränitätsverlust der Bundesrepublik Deutschlands vor.[245] Zum einen sei das Verhältnis zwischen Union und Mitgliedstaaten weiterhin durch das Prinzip der

---

[239] Es handelte sich um zwei Organstreitverfahren durch den Bundestagsabgeordneten Peter Gauweiler (CSU) und die Bundestagsfraktion Die Linke sowie um vier Individualverfassungsbeschwerden von Abgeordneten des Deutschen Bundestages und Privatpersonen.

[240] BVerfGE 123, 267 (370 ff.).

[241] BVerfGE 89, 155, Ls. 8.

[242] BVerfGE 123, 267 (372).

[243] Kleine Staaten wie Malta und Luxemburg entsenden im Verhältnis zu ihrer jeweiligen Bevölkerungsanzahl zu viele Abgeordnete ins Europäische Parlament; vgl. BVerfGE 123, 267 (374 f.).

[244] BVerfGE 123, 267 (371).

[245] *Zimmermann*, JURA 2009, 844 (848).

begrenzten Einzelermächtigung geprägt.[246] Zum anderen würden die Grundsätze der Subsidiarität und der Verhältnismäßigkeit weiterhin wesentliche Elemente mitgliedstaatlicher Autonomie garantieren.[247]

Und drittens legt das Bundesverfassungsgericht in Weiterführung der eigenen Rechtsprechung zum Vertrag von Maastricht[248] fest, dass zentrale Politikbereiche im Einflussbereich der Nationalstaaten zu verbleiben haben.[249] Die Strafrechtspflege wird dabei explizit als ein zentraler Teil diese Kerns nationaler Entscheidungsbefugnisse herausgehoben.[250]

2. *Strafrechtsspezifische Elemente des Lissabon-Urteils*

In den Ausführungen des Bundesverfassungsgerichts spielen insbesondere geänderte bzw. neu hinzugekommene materiell-strafrechtliche Kompetenzen der Europäischen Union eine tragende Rolle. Diese Schwerpunktsetzung geht maßgeblich auch darauf zurück, dass das Bundesverfassungsgericht – in Übereinstimmung mit der Strafrechtswissenschaft – seit Langem die Wichtigkeit der Entscheidungshoheit eines Nationalstaats über die Ausgestaltung des prozessualen und materiellen Strafrechts betont. Dies wird insbesondere im o. g. strafrechtsspezifischen Schonungsgrundsatz greifbar.

Obwohl das Bundesverfassungsgericht die Vorrangwirkung des europäischen Rechts grundsätzlich anerkennt und sich durch die *Ultra-vires*-Kontrolle nur für besondere Fälle eine Letztentscheidungsbefugnis bezüglich der Anwendbarkeit des EU-Rechts vorbehält, verlangt es im Lissabon-Urteil, dass die Kompetenznormen des AEUV zur Harmonisierung des Strafrechts in verfassungskonformer Weise und daher restriktiv auszulegen seien.

Zunächst erkennt das Bundesverfassungsgericht an, dass die Bundesrepublik Deutschland aufgrund des Vorrangs des Unionsrechts, aber ebenso aufgrund völkerrechtlicher Verpflichtungen, grundsätzlich auch im Hinblick auf strafrechtliche Erwägungen gebunden sei und überstaatlichem Recht auf eigenem Territorium zu Geltung und Anwendung verhelfen müsse.[251] Nachdem sich daraus in der Vergangenheit vor allem Konsequenzen für die Herausbildung einer internationalen Strafjustiz zu Völkermord, Verbrechen gegen die Menschlichkeit und Kriegsverbrechen ergeben hätten, würden mit der bundesrepublikanischen Einbindung in die Europäische Union weitere Verpflichtungen einherge-

---

[246] BVerfGE 123, 267 (381 f.).
[247] BVerfGE 123, 267 (383).
[248] BVerfGE 89, 155 (207).
[249] *Zimmermann*, JURA 2009, 844 (849).
[250] BVerfGE 123, 267 (347 f.).
[251] BVerfGE 123, 267 (409) unter Verweis auf BVerfGE 112, 1 (26).

hen, die sich in materiell-strafrechtlicher Weise insbesondere durch den Aufbau des Raums der Freiheit, der Sicherheit und des Rechts zeigen.[252]

Gerade aber weil die anerkannten strafrechtlichen Kooperations- und Harmonisierungsverpflichtungen im europäischen Staatenverbund im Rahmen der ehemaligen intergouvernementalen „dritten Säule" zugenommen hätten, seien die Kompetenzgrundlagen aufgrund „der besonders empfindlichen Berührung der demokratischen Selbstbestimmung durch Straf- und Strafverfahrensnormen […] strikt – keinesfalls extensiv – auszulegen und ihre Nutzung [bedürfe] besonderer Rechtfertigung"[253]. Vor allem das materielle Strafrecht, das die besonders sensible Aufgabe verfolge, über das rechtsethische Minimum in einer Gesellschaft zu entscheiden, dürfe „nicht als rechtstechnisches Instrument zur Effektuierung einer internationalen Zusammenarbeit" genutzt werden.

Die Verpflichtung zur begrenzenden Auslegung des Art. 83 Abs. 1 AEUV folge zudem aus der Beschränkung der Harmonisierungskompetenz des Art. 83 AEUV auf Bereiche besonders schwerer Kriminalität mit typischerweise grenzüberschreitender Dimension.[254] Diese sei überdies deshalb geboten, da durch die Harmonisierung eine Rechtsgemeinschaft daran gehindert werde, auf Basis ihrer eigenen historisch gewachsenen Wertvorstellungen über die Strafbarkeit von Verhaltensweisen und die Verhängung von Strafen zu disponieren.[255] In der Konsequenz durchaus nachvollziehbar, geht das BVerfG davon aus, dass Harmonisierungsakte lediglich auf die grenzüberschreitende Dimension eines Straftatbestandes zielen könnten, um so die grundsätzlich integrationsfeste Strafkompetenz der europäischen Mitgliedstaaten zu achten. Daher sollten etwa lediglich Tatbestandsvarianten und nicht vollständige Deliktsbereiche harmonisiert werden können.[256]

III. Stellungnahme

Das europäische Primärrecht ist zumindest verfassungsähnlich, und dabei gar noch fragmentarischer und lückenhafter als nationalstaatliche Verfassungen, ausgestaltet. Es kann nur sinnvoll angewendet werden, wenn die EU-Institutionen diese Lücken ausfüllen können. Dies hat der EuGH als anerkannte Interpretationsinstanz in der Vergangenheit auch getan.

---

252 BVerfGE 123, 267 (409) unter Verweis auf BVerfGE 113, 273 (296 f.).

253 BVerfGE 123, 267 (410).

254 BVerfGE 123, 267 (412).

255 BVerfGE 123, 267 (412 f.).

256 BVerfGE 123, 267 (412 f.); zustimmend *Böse*, in: Schwarze (Hrsg.), Art. 83 AEUV Rn. 4; überzeugender a. A. sind hingegen *Vogel/Eisele*, in: Grabitz/Hilf/Nettesheim (Hrsg.), 57. EL Aug. 2015, Art. 83 AEUV Rn. 44.

An die obigen Ausführungen zum europäischen Auslegungsprozess anknüpfend ist grundsätzlich davon auszugehen, dass in Streitfragen bei der Ermittlung einer Kompetenzweite grundsätzlich die dynamisch-teleologische Auslegung einer EU-Vorschrift und insbesondere auch topisch-problemorientierte Aspekte im Auslegungsprozess maßgeblich sind und der Effektivitätsgrundsatz (*effet utile*) eine entscheidende Rolle spielt, sodass für eine strikt begrenzende, enge Auslegung in der Regel kein Raum bleibt.[257] Im Interpretationsprozess zum EU-Primärrecht hat der Anspruch auf restriktiv zu verstehende Normen zwar somit regelmäßig keinen Platz. Das heißt jedoch nicht, dass Elemente zum Schutz der mitgliedstaatlichen Souveränität keine Beachtung fänden. Sie kommen lediglich nicht durch nationalstaatlich geprägte Auslegungsmethoden zur Anwendung, sondern finden sich vielmehr bereits im Unionsrecht selbst.[258]

So verständlich die Intention des Bundesverfassungsgerichts in seinem Lissabon-Urteil zur restriktiven Auslegung der Kompetenznorm des Art. 83 Abs. 1 AEUV auch sein mag, so wenig begründbar stellt sie sich in Anbetracht des, auch vom Bundesverfassungsgericht für das europäische Recht grundsätzlich anerkannten,[259] Interpretationsprimats des EuGH dar. Die Forderung nach einer restriktiven Auslegung bei gleichzeitiger Anerkennung der Deutungshoheit des EuGH ist somit als Debattenbeitrag im oben benannten Verfassungsgerichtsdialog zu verstehen.

Dieser Mangel an unmittelbarer EU-rechtlicher Relevanz des Lissabon-Urteils des Bundesverfassungsgerichts lässt sich insbesondere an Folgendem verdeutlichen: Die dynamisch-teleologische Interpretationsmethode zeichnet sich gerade durch ihre funktionale Zielbestimmung aus. Durch eine Orientierung des EuGH am Grundsatz des *effet utile* sind supranationalen Wirksamkeitserwägungen kaum Grenzen gesetzt.[260] Die Fokussierung des Bundesverfassungsgerichts auf die enge Auslegung des Merkmals der grenzüberschreitenden Dimension von Kriminalitätsbereichen oder einzelnen Straftaten durch Beschränkung auf die Harmonisierung ausschließlich transnationaler Tatbestandvarianten ist mit der häufigen und anerkannten Praxis der umfassenden Harmonisierung unvereinbar.[261] Wie bereits oben erörtert,[262] sind die Kriminalitätsbereiche in Art. 83

[257] *Gärditz*, in: Böse/Hatje (Hrsg.), EnzEuR Bd. 9, § 6 Rn. 26 und *Satzger*, in: Streinz (Hrsg.), Art. 83 AEUV Rn. 9, gehen nicht davon aus, dass eine restriktive Auslegung zur Anwendung kommen wird; vgl. insb. auch *Meyer*, Strafrechtsgenese, S. 412.

[258] Vgl. insoweit auch unten, Kap. 3 § 12 D. II.

[259] *Meyer*, Strafrechtsgenese, S. 411 m. w. N.

[260] *Meyer*, Strafrechtsgenese, S. 411.

[261] Vgl. *Vogel/Eisele*, in: Grabitz/Hilf/Nettesheim (Hrsg.), 57. EL Aug. 2015, Art. 83 AEUV Rn. 41, die explizit darauf hinweisen, dass auch minderschwere Computerdelikte aufgrund der Kompetenz des Art. 83 Abs. 1 UAbs. 2 AEUV harmonisierungsfähig sind.

[262] Siehe unten, Kap. 2 § 7 B. III.

Abs. 1 UAbs. 2 AEUV abschließend als solche mit besonderer Schwere und typischerweise grenzüberscheitender Dimension definiert, sodass weder durch eine fortwährende Überprüfung dieser Voraussetzungen noch durch eine restriktive Auslegung der Merkmale eine Kompetenzeingrenzung erfolgen kann.

Möglicherweise wird sich also sowohl in der Breite als auch in der Tiefe des Harmonisierungsvorgehens der Europäischen Union der funktionale und sachbezogene Ansatz mithilfe der dynamisch-teleologischen, am Effektivitätsgrundsatz orientierten Auslegung gegenüber einem restriktiven Ansatz durchsetzen.[263] Jedoch stellt dieses Ergebnis, wie oben bereits gezeigt, lediglich den Beginn eines komplexen Auslegungsvorgangs bezüglich des Unionsrechts und insbesondere von Kompetenznormen dar. Dass am Ende dieses Prozesses eine weite Auslegung von Art. 83 Abs. 1 AEUV und namentlich des Begriffs der Computerkriminalität durch eine besondere Betonung des dynamisch-teleologischen Arguments seitens des EuGH steht, ist letztlich nur eine Vermutung, der in tatsächlicher Hinsicht gewichtige Argumente entgegenstehen. Vor allem die bereits erläuterten Lissabon-Entscheidungen der mitgliedstaatlichen Verfassungsgerichte, die zwar allesamt den Vertrag von Lissabon als vereinbar mit den jeweiligen nationalen Verfassungen einstuften, gleichzeitig aber auf die Notwendigkeit des Erhalts der Verfassungsidentität hinwiesen, werden voraussichtlich den EU-Auslegungsprozess zu Art. 83 AEUV maßgeblich beeinflussen. Dass ihre energischen Rufe nach einer restriktiven Kompetenzausübung bei den EU-Institutionen durchaus wahrgenommen wurden, kann möglicherweise bereits in der Richtlinie 2013/40/EU zur Computerkriminalität erkannt werden.[264]

Zusammenfassend ist festzustellen, dass das Bundesverfassungsgericht mit seiner Kritik und seinen Erwartungen an die EU-Institutionen methodisch nicht an der richtigen Stelle ansetzt. *Meyer* spricht insoweit von einem „fatalen Widerspruch“, dem das Bundesverfassungsgericht unterliegt, indem es einerseits die Auslegungsmethodik des EuGH und den funktionalen Charakter der Kompetenznormen anerkennt, andererseits aber eine restriktive Auslegung der Begriffe „grenzüberschreitende Dimension“ und „besondere Schwere“ fordert.[265] Dies vermag eine Beschränkung der exekutiven und legislativen Maßnahmen der Europäischen Union somit nicht herbeizuführen. Gleichwohl ist die Entscheidung des Bundesverfassungsgerichts zum Vertrag von Lissabon auch für den europäischen Auslegungsprozess relevant und kann entweder auf nachgelagerter Kompetenzausübungsebene oder auf vorgelagerter Begriffsbestimmungsebene einbezogen werden. So wird eine rechtliche Forderung zu einem

---

[263] *Meyer*, Strafrechtsgenese, S. 412.
[264] Im Einzelnen vgl. unten, Kap. 3 § 11.
[265] *Meyer*, EuR 2011, 169 (180 f.).

relevanten Interpretationsgesichtspunkt umgedeutet. Pointiert gesprochen, verkennt das BVerfG zwar in Teilen die EU-rechtliche Methodik, trägt mit seinem Grundtenor allerdings dennoch im Rahmen eines Verfassungsgerichtsdialogs zum Interpretationsergebnis des EuGH bei.

D. Schranken des EU-Primärrechts im Harmonisierungsprozess

Es hat sich herausgestellt, dass eine restriktive Auslegung der Voraussetzungen des Art. 83 Abs. 1 AEUV, „besonders schwere Kriminalität“ und „grenzüberschreitende Dimension“, nicht in Betracht kommt, um die Harmonisierung des Computerkriminalitätsbereichs zu begrenzen.

Möglicherweisen können jedoch die primärrechtlich verankerten Schranken in ausreichender Weise einer uferlosen Harmonisierungskompetenz durch Art. 83 Abs. 1 AEUV vorbeugen. Wäre dies der Fall, könnte über eine gewisse Unbestimmtheit der Kriminalitätsbereiche des Art. 83 Abs. 1 UAbs. 2 AEUV gegebenenfalls hinweggesehen werden, da jene letztlich auf Kompetenzausübungsebene hinreichend eng gefasst würden.

I. Subsidiaritätsprinzip

Hinsichtlich des „Ob“ eines europäischen Tätigwerdens ist dabei zunächst die Kompetenzausübungsschranke des sog. Subsidiaritätsprinzips zu beachten, das in Art. 5 Abs. 1 S. 2, Abs. 3 EUV verankert ist. Für den Fall der geteilten Kompetenz, die den Raum der Freiheit, der Sicherheit und des Rechts gem. Art. 67 ff. AEUV im Allgemeinen und hier den Art. 83 AEUV im Speziellen betrifft, besagt es, dass die Europäische Union von ihrer Kompetenz zur Harmonisierung im Einzelfall nur dann tatsächlich Gebrauch machen darf, wenn die anvisierten Ziele auf Unionsebene besser verwirklicht werden können als auf zentraler, regionaler oder lokaler Ebene innerhalb der Mitgliedstaaten selbst. Im Rahmen des Harmonisierungsvorgangs bedeutet die Berücksichtigung des Subsidiaritätsgrundsatzes, dass die EU-Organe aufgefordert sind, besondere Rechtfertigungs- und Begründungserfordernisse zu erfüllen.[266]

Letztlich heißt dies, dass auch wenn der Begriff der Computerkriminalität im Rahmen der Kompetenznorm des Art. 83 Abs. 1 AEUV weit ausgelegt wird, das Subsidiaritätsprinzip bei Erlass einer Richtlinie einschränkend wirken kann. Insbesondere die Tatsache allerdings, dass ein Tätigwerden bereits dann als erforderlich angesehen wird, wenn auch nur ein Mitgliedstaat nicht von sich

[266] *Hecker*, Europäisches Strafrecht, Kap. 8 Rn. 50; *Zöller*, in: FS Schenke (2011), S. 579 (595).

aus die nötigen Maßnahmen ergreift,[267] schränkt den harmonisierungsbegrenzenden Charakter dieses in der Theorie wichtigen Schutzprinzips nationaler Interessen erheblich ein.

II. Verhältnismäßigkeitsprinzip

Als weitere Kompetenzausübungsschranke ist das Verhältnismäßigkeitsprinzip im Rahmen des Erlasses von Harmonisierungsvorhaben zu berücksichtigen. Es ist in Art. 5 Abs. 1 S. 2, Abs. 4 EUV und in Art. 69 AEUV niedergelegt und hat sich von einem ungeschriebenen europarechtlichen Grundsatz zu einem zwingend zu beachtenden und primärrechtlich kodifizierten Rechtsprinzip entwickelt. Ursprünglich wurde dieser Grundsatz lediglich im Verhältnis zwischen der öffentlichen Gewalt und dem einzelnen Bürger relevant, mittlerweile aber handelt es sich bei dem EU-rechtlichen Verhältnismäßigkeitsgrundsatz um ein Rechtsprinzip, das zumindest vorwiegend das Verhältnis zwischen der Europäischen Union und den Mitgliedstaaten bestimmt.[268]

Den Kerngedanken des europäischen Verhältnismäßigkeitsgrundsatzes bildet seit dem Vertrag von Maastricht die aus dem Verfassungs- und Verwaltungsrecht bekannte Formel, dass Maßnahmen der Union „nicht über das für die Erreichung dieser Ziele erforderliche Maß hinaus[gehen]"[269] sollen. Dafür sind alle drei bekannten Stufen der Verhältnismäßigkeit heranzuziehen: Geeignetheit, Erforderlichkeit und Angemessenheit.[270] Bezüglich der Geeignetheit ist relevant, dass diese sich unmittelbar auf das Ziel der Maßnahme und nicht auf möglicherweise übergreifende Unionsziele bezieht[271] und dass den politischen Organen der Union ein sehr weiter Ermessensspielraum zugestanden wird, sodass nur offensichtlich ungeeignete Maßnahmen primärrechtswidrig sind.[272] Unter Beachtung der Erforderlichkeit ist „inhaltlich wie formal" diejenige geeignete Maßnahme zu wählen, welche die Handlungsspielräume der Mitgliedstaaten am wenigsten einschränkt. Als Gradmesser kommen dafür etwa die

---

[267] *Hecker*, Europäisches Strafrecht, Kap. 8 Rn. 50; *Satzger*, Europäisierung des Strafrechts, S. 447.

[268] Vgl. EuGH, Rs. 41/79, Slg. 1980, 01979, Rn. 21 – *Testa/Bundesanstalt für Arbeit*; Rs. 265/87, Slg. 1989, 2237, Rn. 21 ff. – *Schräder/Hauptzollamt Gronau*; Rs. C-331/88, Slg. 1990, I-4023, Rn. 12 ff. – *The Queen/Fedesa*; Rs. C-133/93, Slg. 1994, I-4863, Rn. 41 – *Crispoltoni*; siehe dazu auch insb. *Kadelbach* in: von der Groeben/Schwarze/Hatje (Hrsg.), Art. 5 EUV Rn. 49.

[269] Art. 3 lit. b EGV Maastrichter Fassung, zuletzt Art. 5 UAbs. 3 EGV.

[270] *Grupp/Schäder*, EWS 1993, 27 ff.; *Schwarze*, Europäisches Verwaltungsrecht Bd. 2, S. 661 ff.

[271] *Kadelbach*, in: von der Groeben/Schwarze/Hatje (Hrsg.), Art. 5 EUV Rn. 51.

[272] EuGH, Rs. C-84/94, Slg. 1996, I-5755, Rn. 58 – *Arbeitszeitrichtlinie*; Rs. C-365/08, Slg. 2010, I-4341, Rn. 31 – *Agrana Zucker*.

Wirkungsintensität der Maßnahme, das Harmonisierungsniveau, die Regelungstiefe oder auch die entstehenden finanziellen Belastungen in Betracht.[273] Obwohl die Angemessenheit in Art. 5 Abs. 3 EUV nicht explizit als Prüfungsmaßstab genannt ist, was ursprünglich zu Differenzen hinsichtlich ihrer EU-rechtlichen Relevanz führte,[274] fordert auch das auf den Verhältnismäßigkeitsgrundsatz anwendbare Subsidiaritätsprotokoll in Art. 5 S. 5 ein „angemessenes Verhältnis zu dem angestrebten Ziel".

III. Strafrechtlicher Schonungsgrundsatz

Schließlich spielt in diesem Rahmen auch noch der bereits weiter oben angesprochene sog. strafrechtliche Schonungsgrundsatz[275] eine Rolle, wonach den EU-Mitgliedstaaten auch bei Erlass von Richtlinien ausreichende Spielräume im Umsetzungsprozess belassen werden müssen. Daher dürfen etwa weder konkrete Straftatbestände ausformuliert noch verpflichtende Rechtsfolgen eingefordert werden.[276] In den bisherigen strafrechtlichen EU-Richtlinien zeigt sich eine Beachtung dieses Gebots beispielsweise in dem Gebrauch von Mindest-Höchststrafen anstelle von verpflichtenden Strafvorgaben an die Mitgliedstaaten. Auch die „Tatbestände" in den Richtlinientexten sind eindeutig als Vorschläge für die nationale Umsetzung formuliert.

IV. Stellungnahme

Weder für die Voraussetzung der besonderen Schwere noch über diejenige der grenzüberschreitenden Dimension können die genannten Primärrechtsgrundsätze dem Begriff der Computerkriminalität allerdings hinreichende Grenzen setzen.

Grundsätzlich sind die Kompetenzausübungsschranken geeignet, um uferlose Harmonisierungen und Überdehnungen der Kompetenznormen zu verhindern. Grenzüberschreitende Straftaten, die im Bereich der Computerkriminalität oftmals vorliegen, sind allerdings selbst unter strenger Beachtung der hier aufgeführten Prinzipien regelmäßig effektiver auf transnationaler Ebene oder zumindest durch zwischenstaatliche Kooperationen zu bekämpfen und aufzu-

---

[273] *Bast*, in: Grabitz/Hilf/Nettesheim (Hrsg.), 57. EL Aug. 2015, Art. 5 EUV Rn. 75; *Calliess*, in: ders./Ruffert (Hrsg.), Art. 5 EUV Rn. 55.

[274] EuGH, Rs. C-84/94, Slg. 1996, I-5755, Rn. 57 – *Arbeitszeitrichtlinie* beispielsweise nennt nur die Geeignetheit und die Erforderlichkeit; siehe aber auch EuG, Rs. T-390/08, Slg. 2009, II-3967, Rn. 66 – *Bank Melli Iran/Rat*.

[275] Vgl. bereits oben, Kap. 1 § 2 A. VI.

[276] Vgl. *Hecker*, Europäisches Strafrecht, Kap. 8 Rn. 55; *Satzger*, Internationales und Europäisches Strafrecht, § 9 Rn. 27; *Zöller*, in: FS Schenke (2011), S. 579 (597).

klären. Ein weitgehend harmonisiertes materielles Strafrecht schafft die dazu nötige Grundlage. Subsidiaritäts- und Verhältnismäßigkeitsgrundsatz sowie auch das Schonungsgebot könnten daher allenfalls durch die Aufspaltung von Strafnormen in transnationale und nationale Tatbestandsalternativen umfassend gewahrt werden. Eine solche Konstellation erscheint jedoch unpraktikabel und vermutlich sogar nur schwerlich mit verfassungsrechtlichen Bestimmtheitsgrundsätzen vereinbar, sodass letztlich auch bei Beachtung der genannten Grundsätze eine umfassende Harmonisierung primärrechtmäßig sein dürfte.

Hinsichtlich der Voraussetzung der besonderen Schwere stellt sich die Situation etwas anders dar. Hierbei scheitert eine Begrenzung nicht an der Praktikabilität einer Konzentration auf derartige Delikte unter Ausschluss von minderschwerer Kriminalität. Dennoch können die Kompetenzausübungsschranken auch hier keine Begrenzung der Harmonisierungsermächtigung begründen. Weder Subsidiaritätsprinzip und Verhältnismäßigkeitsgrundsatz noch das Schonungsgebot sprechen gegen eine EU-Kompetenz zur Harmonisierung auch minderschwerer Computerdelikte. Die Signifikanz einer Straftat oder generell einer EU-rechtlichen Regelungsmaterie stellt keine Beurteilungsgröße bei der Abgrenzung zwischen nationalstaatlichen und unionalen Zuständigkeiten dar. Auch geringfügige Straftaten können gegebenenfalls effektiver in transnationaler Weise bekämpft werden.

Wie schon eine restriktive Auslegung der Voraussetzungen der „besonderen Schwere“ und der „grenzüberschreitenden Dimension“ der Kriminalitätsbereiche vermögen es auch die Kompetenzausübungsschranken des europäischen Primärrechts somit nicht, eine hinreichende Begrenzung der Kompetenzen zur materiellen Strafrechtsangleichung herbeizuführen, oder auch nur eine exakte Klärung der harmonisierungsfähigen Kriminalitätsbereiche, inklusive der Computerkriminalität, zuzulassen.

Insbesondere der Umstand, dass nahezu jegliche Form von Computerdelikten (unabhängig davon, welche Begriffsdefinition man letztlich als Maßstab nimmt) sog. Distanzdelikte[277] darstellt, und daher bei einem zusammenwachsenden Wirtschafts- und Gesellschaftsmodell wie der Europäischen Union potenziell immer mehrere Rechtskreise und -systeme berührt, macht die Argumentation für ein gleichwertig aussichtsreiches mitgliedstaatliches Vorgehen nahezu unmöglich.

---

[277] Von Distanzdelikten spricht man, wenn Handlungs- und Erfolgsort auseinanderfallen; weiterführend zur Thematik siehe *Heinrich*, in: FS Weber (2004), S. 91 ff.; vgl. auch *Satzger*, Internationales und Europäisches Strafrecht, § 5 Rn. 18. Siehe auch *Meier*, in: Beck/ders./Momsen (Hrsg.), Cybercrime, S. 93 (95 f.), der deutlich macht, dass die Gefährlichkeit der Internetkriminalität hauptsächlich auf der Tatsache beruht, dass es sich regelmäßig um Distanzkriminalität handele.

§ 8 Computerkriminalität als europäischer Rechtsbegriff

Es hat sich gezeigt, dass weder auf Kompetenzbegründungs- noch auf Kompetenzausübungsebene eine Eingrenzung der materiell-strafrechtlichen EU-Harmonisierungsermächtigungen zu erreichen ist. Einerseits führt die europapolitisch gewünschte und mitgliedstaatlich akzeptierte Kraft der dynamisch-teleologischen und am *effet utile* orientierten Auslegungsmethodik dazu, dass eine ergebnisoffene Überprüfung des Kriminalitätsbereichs der Computerkriminalität, auf seine „besondere Schwere" und „grenzüberschreitende Dimension" hin, leerlaufen muss. Das liegt vor allem daran, dass das Vorliegen dieser beiden Voraussetzungen gesetzlich vermutet wird. Andererseits sind auch die primärrechtlichen Kompetenzausübungsschranken nicht hinreichend geeignet, tatsächliche Harmonisierungsgrenzen zu ziehen. Erstens ist die grenzüberschreitende Dimension einer Vielzahl von Computerdelikten kaum abzustreiten, sodass im Regelfall Subsidiaritätseinwände ohne Wirkung bleiben. Zweitens sind bei der Verhältnismäßigkeitsprüfung die Ziele des Unionsrechts als Referenzgröße heranzuziehen, sodass eine Entscheidung letztlich wieder vom begrifflichen Verständnis der Kriminalitätsbereiche abhängt. Nur dann kann schließlich beurteilt werden, ob das gewählte Mittel zur Zielerreichung geeignet, erforderlich und angemessen ist. Subsidiaritätsprinzip und Verhältnismäßigkeitsgrundsatz mögen daher zwar durchaus konkrete Umsetzungsakte verhindern, können allerdings nicht für eine ausreichende Klarheit bei der Bestimmung der allgemeinen Harmonisierungskompetenz des Art. 83 Abs. 1 AEUV sorgen.

Um also, auch mit dem Bundesverfassungsgericht, sowohl eine uferlose Strafrechtskompetenz der EU als auch die überbordende Nutzung des Strafrechts zur Flankierung und Effektuierung anderer Rechts- und Politikbereiche zu verhindern, ist eine begriffliche Klarstellung der Kriminalitätsbereiche des Art. 83 Abs. 1 UAbs. 2 AEUV weiterhin notwendig.

Es gilt also den Kompetenzbereich einerseits klar zu umreißen, um zumindest rudimentären Bestimmtheitserfordernissen gerecht zu werden und gleichzeitig dem Grundsatz einer umfassenden Harmonisierungsermächtigung nicht zu widersprechen. Dazu muss einen gedanklichen und prüfungstechnischen Schritt weiter vorne angesetzt werden. Wie sich gezeigt hat, ist der Begriff der Computerkriminalität bereits für sich genommen, unabhängig von seiner primärrechtlichen Verankerung, so unscharf, dass eine restriktive Begriffseinordnung gerechtfertigt ist.[278] Eine solche mag zwar ganz ähnlich klingen wie eine restriktive Auslegung der Voraussetzungen von Art. 83 Abs. 1 AEUV, wie sie

[278] Dazu u. a. *Sieber*, in: Delmas-Marty/Pieth/ders. (Hrsg.), Harmonising Criminal Law, S. 127 (128 f.).

u. a. das Bundesverfassungsgericht fordert. Der im Folgenden skizzierte Ansatz geht aber einen anderen und mit der EU-rechtlichen Methodik besser zu vereinbarenden Weg. Es wird nicht vom weiten Computerkriminalitätsbegriff ausgegangen, wie er sich in den vergangenen Jahrzehnten herausgebildet hat, um daraufhin dessen problematische Weite entgegen der EU-rechtlichen Auslegungsmethodik durch Beschränkung auf besonders schwere und grenzüberschreitende Fälle einzudämmen. Stattdessen respektieren die folgenden Ausführungen sowohl die Vermutung des Vorliegens der Voraussetzungen des Art. 83 Abs. 1 AEUV als auch die umfassende Harmonisierungskompetenz der Europäischen Union für einen Rechtsbereich.

Dazu wird der Begriff der Computerkriminalität *konzentriert* und infolgedessen zu einem europäischen Rechtsbegriff. An dieser Stelle wird also davon ausgegangen, dass der Computerkriminalitätsbegriff in Art. 83 Abs. 1 UAbs. 2 AEUV *nicht* deckungsgleich mit dem herkömmlichen Computerkriminalitätsbegriff sein *kann*. Diese Einschätzung geht darauf zurück, dass es sich bei der Computerkriminalität eben nur dann um einen Bereich besonders schwerer Kriminalität mit grenzüberschreitender Dimension handeln kann, wenn nicht sämtliche Bereiche herkömmlicher Definitionen eingeschlossen sind.[279] Im Unterschied zu Befürwortern einer Überprüfung der Sekundärrechtsakte anhand der Voraussetzungen des Art. 83 Abs. 1 AEUV geht der hier vorgestellte Ansatz mit der herrschenden Ansicht davon aus, dass die Kriminalitätsbereiche anhand eines Typisierungsmodells zur besonders schweren Kriminalität mit grenzüberschreitender Dimension und damit zum Harmonisierungsobjekt geworden sind. Folglich besteht durch ein Zusammenspiel mit dem Grundsatz der umfassenden Harmonisierungskompetenz für einen Rechtsbereich durchaus auch eine Kompetenz zur Angleichung von Straftaten, die jene Voraussetzungen nicht im Einzelnen erfüllen. Der Unterschied zu einer nachträglichen Überprüfung des Bereichs der Computerkriminalität, wie sie oben bereits mit der h. A. verworfen wurde,[280] liegt hingegen darin, dass die Voraussetzungen des Art. 83 Abs. 1 UAbs. 1 AEUV nicht dazu herangezogen werden, die in Art. 83 Abs. 1 UAbs. 2 AEUV definierten Kriminalitätsbereiche ergebnisoffenen Überprüfungen zu unterziehen. Stattdessen werden die Vorrausetzungen zur begrifflichen Auslegung der Computerkriminalität i. S. d. EU-Primärrechts verwendet.

Es wird also versucht, aus der Masse aller Delikte, die bislang als Computerkriminalität i. w. S. klassifiziert worden sind, diejenigen Bereiche herauszu-

---

[279] Auch *Fahey*, EJRR 2014, 46 (47) weist darauf hin, dass der Computerkriminalitätsbegriff weit oder eng verstanden werden kann, eine eigenständige Definition für das Unionsrecht jedoch bislang nicht bestehe und daher lediglich auf die Begriffsannäherungen der Cybercrime Convention (ETS Nr. 185) zurückgegriffen werde.

[280] Siehe oben, Kap. 2 § 7 B. III.

destillieren, denen typischerweise eine besondere Schwere und grenzüberschreitende Dimension innewohnt. Am Ende dieser Untersuchung sollen dann Kriterien zur Bestimmung eines primärrechtskonformen und damit europäischen Rechtsbegriffs der Computerkriminalität stehen.

Dieses Vorgehen wird schließlich auch dem Rangverhältnis zwischen EU- und mitgliedstaatlichem Recht sowie der EU-rechtlichen Interpretationsmethodik optimal gerecht. Das liegt daran, dass zum Schutz der mitgliedstaatlichen Autonomie des materiellen Strafrechts eben nicht verfassungsrechtliche Kriterien auf nationaler Ebene herangezogen werden, wie es das Bundesverfassungsgericht teilweise macht. Stattdessen kommt es zur konsequenten Anwendung der primärrechtlichen Voraussetzungen des Art. 83 Abs. 1 AEUV im Rahmen eines EU-rechtlichen Auslegungsvorgangs.

A. Grundbedingungen der primärrechtskonformen Begriffsbestimmung

Zunächst sind dafür ein gemeinsamer Nenner und gemeinsame Charakteristika von Deliktsgruppen zu identifizieren, die regelmäßig mit dem Begriff der Computerkriminalität assoziiert werden.[281] Die nach weitestem Begriffsverständnis umfassten Unterbereiche (1) Angriffe auf computergestützte Systeme, (2) unter Verwendung von Computern oder anderer moderner Endgeräte begangene klassische Delikte, (3) inhaltsbezogene Delikte und (4) Delikte gegen das Urheberrecht erfüllen in ihrer Gesamtheit weder den ersten noch den zweiten Aspekt, wenn man nicht bereits die irgendwie geartete Beteiligung eines Computers im Gesamtprozess der Straftat als ausreichenden gemeinsamen Nenner und verbindendes Charakteristikum erachtet. Eine solche Klassifizierung kann aber lediglich für banale Aussagen über die weitverbreitete Nutzung moderner Technologien, und damit auch deren Verwendung durch Kriminelle, hilfreich sein.

Schließlich werden Kriminalitätsbereiche auch ansonsten regelmäßig nicht in derartiger Weise klassifiziert, sodass etwa „Messerkriminalität" oder „Autokriminalität" nicht als geeignete Kategorien erachtet werden. Stattdessen werden Oberbegriffe gewählt, die eine besondere Gefährdungssituation verdeutlichen, um Straftaten zu gruppieren. Der Kriminalitätsbereich der Straßenverkehrsdelikte beispielsweise umfasst Straftaten, die jeweils Ausdruck der besonderen Gefahren des Straßenverkehrs sind.

Den Interessen eines zusammenwachsenden Gesellschafts-, Wirtschafts- und Rechtsraums, wie der Europäischen Union, entspricht bezüglich einer Rechts-

[281] Vom Ansatz her so auch *Sieber*, in: Delmas-Marty/Pieth/ders. (Hrsg.), Harmonising Criminal Law, S. 127 (131), der allerdings andere Schlüsse daraus zieht.

angleichung im Computerstrafrecht allerdings vielmehr die Identifizierung von – die einzelnen Delikte verbindenden – Spezifika, die nicht nur die durch moderne Technologien erweiterte Gefahrenlage abbilden, sondern tatsächlich neuartige Begehungsmodalitäten und Angriffsobjekte miteinander *vereinen*. Welche Merkmale machen bestimmte Deliktsgruppen aus dem Bereich der Computerkriminalität i. w. S. also sowohl so bedrohlich, dass man sie als der besonders schweren Kriminalität zugehörig einordnen muss, als auch gleichzeitig typischerweise grenzüberschreitend, sodass sie regelmäßig ausschließlich oder zumindest effektiver im europäischen Verbund zu bekämpfen sind?

B. Klassifizierung anhand von Begehungsmodalitäten

Nach den klassischen Begriffsbestimmungen nehmen Computerdelikte, die sich durch Computer(systeme) als Angriffsmittel auszeichnen, einen wesentlichen Bereich ein, da sie die Begehung klassischer Delikte, inhaltsbezogener Delikte und urheberrechtsbezogener Delikte gleichsam umfassen. In der Harmonisierungspraxis der Europäischen Union spielen diese Bereiche bis dato zwar keine Rolle, ein Grund, jene mit dieser Begründung aus der Harmonisierungskompetenz herauszunehmen, wird darin allerdings regelmäßig nicht gesehen.[282] Insbesondere der Verweis auf die Cybercrime Convention in den bisherigen Harmonisierungsinstrumenten[283] deutet auf die grundsätzliche Aufgeschlossenheit des EU-Gesetzgebers zur Angleichung aller darin aufgeführten Bereiche hin.

Einschränkend wird allerdings vorgebracht, dass zumindest ein tatbestandlicher Bezug zu Computersystemen oder -daten bestehen muss, sodass etwa die Vollharmonisierungen des Urkundenstrafrechts oder Medienstrafrechts nicht auf die Kompetenzgrundlage des Art. 83 Abs. 1 UAbs. 2 AEUV gestützt werden könnten, auch wenn empirische Analysen nahelegten, dass Urkundenstraftaten bzw. Mediendelikte häufig oder typischerweise durch Verwendung von Computern begangen würden.[284]

Diese Beschränkung verdeutlicht einen sehr interessanten Aspekt. Sie erscheint zwar einerseits einleuchtend, da einer Vollharmonisierung auf Grundlage von Art. 83 Abs. 1 UAbs. 2 AEUV nahezu sämtlicher Strafrechtsbereiche, die auch mithilfe von Computern begangen werden können, nach allgemeiner Auffassung vorzubeugen ist. Jedoch zeigt sie andererseits auch ein maßgebli-

---

[282] *Vogel/Eisele*, in: Grabitz/Hilf/Nettesheim (Hrsg.), 57. EL Aug. 2015, Art. 83 AEUV Rn. 62.

[283] Rahmenbeschluss 2005/222/JI, ABl. L 69 v. 16.3.2005, Erwägungsgrund 7; Richtlinie 2013/40/EU, ABl. L 218 v. 14.8.2013, Erwägungsgrund 15.

[284] *Vogel/Eisele*, in: Grabitz/Hilf/Nettesheim (Hrsg.), 57. EL Aug. 2015, Art. 83 AEUV Rn. 62.

ches Problem eines solch weiten Verständnisses von Computerkriminalität als Harmonisierungsbereich auf. Den Gedanken fortführend wären dann nämlich viele Deliktsbereiche nur teilweise, also hinsichtlich einer computergestützten Begehung herkömmlicher, inhaltsbezogener und gegen das Urheberrecht gerichteter Straftaten, von der Harmonisierungskompetenz des Art. 83 Abs. 1 UAbs. 2 AEUV umfasst und einer Angleichung zugänglich. Während das in relativ klar abgrenzbaren Fällen, wie etwa dem Computerbetrug nach § 263a StGB noch möglich erscheint, ist kaum ersichtlich, warum computergestützte und analoge Inhaltsdelikte unterschiedlich zu beurteilen sein sollten. Auch wenn die EU also ihre Kompetenz nicht überdehnt und eventuell sogar lediglich rein transnationale Sachverhalte harmonisieren würde, könnten die europäischen Mitgliedstaaten auf diese Weise implizit dazu gedrängt werden, jeweils direkt den gesamten Deliktsbereich zu harmonisieren, um ein Durcheinander innerhalb der strafrechtlichen Normen zu verhindern.[285]

Ginge man davon aus, dass die Harmonisierungskompetenz der Europäischen Union im Bereich der Computerkriminalität regelmäßig dann gegeben ist, wenn Computer(systeme) als Begehungsmittel eingesetzt werden, kann es zu durchaus paradoxen Situationen im mitgliedstaatlichen Strafrecht kommen. Die Orientierung eines Kriminalitätsbereichs an einem Tatwerkzeug führt nämlich dazu,[286] dass es bei der Regulierung konkreter Straftaten regelmäßig zu Überschneidungen mit anderen Kriminalitätsbereichen kommt.

Bei Kriminalitätsbereichen, die jeweils der Harmonisierungskompetenz aus Art. 83 Abs. 1 AEUV unterfallen, ist das weniger problematisch.[287] Anders stellt sich die Situation jedoch dar, wenn Straftaten sowohl dem Bereich der Computerkriminalität als auch einem Kriminalitätsfeld zuzurechnen wären, das nicht vom Kompetenzbereich des EU-Gesetzgebers umfasst ist. Auf diese Weise würden Inkongruenzen innerhalb des betroffenen Kriminalitätsfelds ge-

---

[285] In ähnlicher Weise erkennt *Nuotio*, in: Dubber/Hörnle (Hrsg.), Criminal Law, S. 1115 (1128), diesen sehr weitreichenden Einfluss des Strafrechts der EU auf die Systematik des mitgliedstaatlichen Strafrechts; auch *Summers u. a.*, EU Criminal Law, S. 277, sehen die möglichen Auswirkungen von EU-Instrumenten auf rein nationale Sachverhalte, wenn Computer und das Internet ganz generell mit einer transnationalen Begehungsweise in Verbindung gebracht werden.

[286] *Brenner*, Cybercrime, S. 9, weist ebenfalls darauf hin, dass sich der Bereich der Computerkriminalität – sie spricht freilich von „Cybercrime" – weitestgehend nur durch die Nutzung von Computern zur Tatbegehung unterscheide und es sich damit größtenteils um ganz klassische Straftaten handele.

[287] Die Verbreitung von Kinderpornografie über das Internet fällt beispielsweise sowohl in den Kriminalitätsbereich der Computerkriminalität als auch in denjenigen des Menschenhandels und der sexuellen Ausbeutung von Frauen und Kindern. Abgrenzungsschwierigkeiten wiegen demgemäß nicht so schwer; vgl. dazu auch unten, Kap. 3 § 10.

schaffen, sodass sich die mitgliedstaatlichen Gesetzgeber dazu genötigt fühlen könnten, im Sinne einer einheitlichen Rechtsordnung den eigentlich nicht harmonisierungsfähigen Kriminalitätsbereich ebenfalls anzupassen. Regelungen zur computergestützten Verbreitung von Beleidigungen würden bei einer rein computerbezogenen Umsetzung in deutsches Strafrecht dazu führen, dass möglicherweise eine Aussage nur deswegen mit Strafbarkeit bedroht ist, weil sie unter Verwendung eines Computers getätigt wird, während die öffentliche und mündliche Aussage straffrei bliebe. Auf diesem Wege könnten unscharfe Harmonisierungskompetenzen eine massive Ausstrahlungswirkung auf andere, bislang harmonisierungsfeste, Strafrechtsmaterien entwickeln.

Dieses mitgliedstaatliche Vorgehen könnte unter Umständen bei Beachtung strafrechtlicher Bestimmtheitserfordernisse sogar notwendig werden. Eine Vorhersehbarkeit der drohenden Strafbarkeit und Strafandrohung, könnte andernfalls schwerlich möglich sein, insbesondere durch einen vermehrt entstehenden fließenden Übergang zwischen analogen und digitalen Tätigkeiten. Eine solche Entwicklung Richtung Vollharmonisierung auch nicht digitaler Kriminalitätsfelder „durch die Hintertür“ gilt es allerdings zu verhindern.

C. Klassifizierung anhand von Angriffsobjekten

Dass sich die Europäische Union bisher mit ihren Harmonisierungen auf Grundlage der Computerkriminalitätskompetenz aus Art. 83 Abs. 1 UAbs. 2 AEUV größtenteils auf Deliktsbereiche beschränkt hat,[288] die Daten, Computer oder Computernetzwerke als Angriffsobjekte schützen, ist durchaus zu begrüßen, jedoch nicht ausreichend für eine Begriffseingrenzung. Insbesondere ist die digitale Komponente des Angriffs herauszustellen, sodass analoge Beeinträchtigungen von Daten, Computern oder Computernetzwerken nicht gleichsam vom Harmonisierungsbegriff der Computerkriminalität erfasst werden. Eine auf den ersten Blick problematische Kategorie stellen hierbei diejenigen Angriffe auf Computer und Informationssysteme dar, die nicht über ein Intranet oder das Internet verübt werden, sondern stattdessen durch die Verbindung über USB-Sticks oder andere geeignete Datenträger. Bei abstrahierender Betrachtung werden diese Sachverhaltskonstellationen allerdings ebenfalls den digitalen Angriffsmodalitäten zuzurechnen sein, da die analoge Steckverbindung für sich genommen keine schädlichen Auswirkungen hat. Erst die lokale und digitale Verbindung, die gewissermaßen ein kleines Netzwerk zwischen Datenträger und Computer(system) aufbaut, kann somit vom Begriff umfasst sein.

[288] Dazu im Einzelnen sogleich unten, Kap. 3 § 11.

Letztlich zeigt dies aber, dass auch eine Klassifizierung ausschließlich anhand des Angriffsobjekts gewisse Unschärfen bei der Bestimmung des Computerkriminalitätsbegriffs hinterlässt.

D. Entwicklung eines netzwerkspezifischen Computerkriminalitätsbegriffs

Auch unter Anerkennung der politischen Dimension des EU-Kompetenzrechts und der damit einhergehenden, notwendigen begrifflichen Offenheit, um auf zukünftige Entwicklungen reagieren zu können, indem u. a. anhand der dynamisch-teleologischen Auslegungsmethode Anpassungen vorgenommen werden, kann der Begriff der Computerkriminalität in Art. 83 Abs. 1 UAbs. 2 AEUV nicht in derjenigen Weite verstanden werden, welche die strafrechtliche Literatur ihm gemeinhin zuschreibt. Stattdessen ist ein genuin unionsrechtlicher Computerkriminalitätsbegriff zu entwickeln.

I. Grundannahmen

Die Aufgabe eines Kompetenzkatalogs ist zwar nicht die punktgenaue Regelung zur Umsetzung durch Richtlinien oder Verordnungen, sondern die Absteckung von Betätigungsfeldern für den europäischen Normgeber. Jedoch ist nur dann dem Prinzip der begrenzten Einzelermächtigung ausreichend Rechnung getragen, wenn zumindest die Zuschreibung von Kompetenzen umrissen ist und nicht die Möglichkeit geschaffen wird, durch Begriffsausdehnungen sämtliche strafrechtlichen Lebenssachverhalte unionsweit anzugleichen.

Diese Gefahr droht allerdings durch die Anwendung des weiten Begriffs der Computerkriminalität, wie ihn die Cybercrime Convention vorgibt, auf die sich die Europäische Union in ihren bisherigen Harmonisierungsmaßnahmen auch bezieht, obwohl sie ihre Anstrengungen bislang noch auf einen engen Bereich fokussiert. Anders als die offene völkerrechtliche Vereinbarung des Europarats, ist eine Nichtumsetzung der Harmonisierungsmaßnahmen nach Art. 83 AEUV nur unter Anwendung des Notbremsemechanismus des Art. 83 Abs. 3 AEUV möglich und damit deutlich voraussetzungs- und folgenreicher.[289] Daher ist einem unbegrenzten Gebrauch einer Kompetenznorm entgegenzutreten, indem jene so ausgelegt wird, dass auf ihr basierende Sekundärrechtsakte mit dem geltenden Recht vereinbar sind. Hierzu bedarf es gewisser Annahmen, die einer tauglichen Computerkriminalitätsdefinition zugrunde zu legen sind:

---

[289] Bezüglich des Notbremseverfahrens gem. Art. 83 Abs. 3 AEUV sei auf Kap. 3 § 12 D. II. 2. verwiesen.

Erstens ist die Auslegung des Computerkriminalitätsbegriffs zumindest in seiner unionsrechtlichen Ausprägung anhand EU-rechtlicher Auslegungsgrundsätze und innerhalb des Unionsrechts durchzuführen, um dessen Vorrang gegenüber mitgliedstaatlichem (Verfassungs-)Recht Rechnung zu tragen.

Zweitens ist nach verständiger Würdigung kaum davon auszugehen, dass sämtliche Straftaten, die regelmäßig unter den Begriff der Computerkriminalität subsumiert werden, auch tatsächlich besonders schwere und typischerweise grenzüberschreitende Kriminalität darstellen.[290]

Drittens ist mit der herrschenden Ansicht eine nachträgliche Eingrenzung der Kompetenzgrundlage, bzw. eine Überprüfung der Sekundärrechtsakte, anhand der in Art. 83 Abs. 1 UAbs. 1 AEUV genannten Voraussetzungen abzulehnen. Denn schließlich *ist* die Computerkriminalität *per definitionem* unionsrechtlich eine besonders schwere und typischerweise grenzüberschreitende Kriminalitätserscheinung.[291]

Viertens gibt das Unionsrecht integrationsbremsende, oder präziser ausgedrückt, integrationskonkretisierende Grundsätze vor, die nicht erst die Kompetenzausübung, sondern bereits die Kompetenzbegründung beeinflussen. Das Subsidiaritätsprinzip, der Verhältnismäßigkeitsgrundsatz sowie die Abgrenzung zur Kompetenz-Kompetenz gestalten schon die primärrechtliche Auslegung der Kompetenznormen. Androhungen von *Ultra-vires*-Kontrollverfahren oder die Anmahnung einer restriktiven Auslegung der Begrifflichkeiten im strafrechtlichen Kompetenzrecht durch mitgliedstaatliche Verfassungsgerichte sind demgemäß übereilt.

Aus der Beachtung dieser Annahmen ergeben sich zwei Konsequenzen. Die Vorrausetzungen des Art. 83 Abs. 1 UAbs. 1 AEUV (besonders schwere und typischerweise grenzüberschreitende Kriminalität) sind *nicht* zur Rechtmäßigkeitskontrolle von kompetenzausübenden Sekundärrechtsakten heranzuziehen. Allerdings sind sie selbstverständlich in Kombination mit dem unionsrechtlich verankerten Subsidiaritätsprinzip bei der Begriffsbestimmung relevant.

Plastisch: Unionsrechtlich kann im Rahmen von Art. 83 Abs. 1 UAbs. 2 AEUV nur diejenige Computerkriminalität gemeint sein, die sowohl besonders schwer als auch typischerweise grenzüberschreitend ist. Dieses Begriffsverständnis kann und wird sich nach den vorangegangenen Untersuchungen von den klassischen Definitionen der Computerkriminalität unterscheiden. Obwohl die folgende Begriffsbestimmung enger und restriktiver sein wird als die o. g. klassischen Definitionen, ist diese Eingrenzung nicht auf verfassungsrechtliche For-

---

[290] Für die Gesamtheit der auf Art. 83 Abs. 1 AEUV beruhenden Rechtsakte vgl. insoweit auch *Meyer*, Strafrechtsgenese, S. 410.

[291] Vgl. statt vieler hier nur: *Zerdick*, in: Lenz/Borchardt (Hrsg.), Art. 83 AEUV Rn. 6.

derungen der Mitgliedstaaten zurückzuführen,[292] *sondern ergibt sich, wie eben gezeigt, unmittelbar aus einer konsequenten Anwendung unionsrechtlicher Grundsätze.*

II. Netzwerkspezifische Computerkriminalität

Ein unionsrechtskonformer Begriff der Computerkriminalität muss demnach so gefasst sein, dass er dem EU-rechtlichen Subsidiaritätsprinzip und den, jenes konkretisierenden, Voraussetzungen des Art. 83 Abs. 1 UAbs. 1 AEUV entspricht. Die herrschende Ansicht zum Computerkriminalitätsbegriff unter Heranziehung phänomenologischer Gesichtspunkte kann diesen Maßstäben nicht gerecht werden.

Zieht man die Grenze jedoch anhand der Beurteilung, ob *sowohl* das Angriffsmittel *als auch* das Angriffsziel der kriminellen Handlung ein Computer oder ein Computernetzwerk ist, wird man einerseits den Voraussetzungen des Art. 83 Abs. 1 AEUV und andererseits den Notwendigkeiten transnationaler Strafverfolgung gerecht. Zwar bleiben auch dann durchaus rein nationale Delikte und solche mit geringerer Intensität von der Definition umfasst. Dies ist jedoch schlechterdings unvermeidbar, wenn Kriminalitätsbereiche gebildet werden. Letztlich trägt dies auch dem Grundsatz einer umfassenden Harmonisierung Rechnung und wirkt gleichzeitig einem inkonsistenten Nebeneinander von harmonisierten und rein nationalen Sachverhaltsvarianten entgegen. Dennoch liegen bei dieser Definition tatsächlich ein gemeinsamer Nenner und gemeinsame Charakteristika vor, die den Deliktsbereich von anderen Kriminalitätsfeldern unterscheidbar machen. Andersfalls würde, wie gezeigt, lediglich auf die „Beteiligung eines Computers am Tatgeschehen" abgestellt. Viele Straftaten, die bislang als Computerstraftaten bezeichnet werden, würden bei dem hier vertretenen Verständnis vom Begriff der Computerkriminalität nicht mehr umfasst betrachtet.

Die Notwendigkeit einer begrifflichen Neufassung ergibt sich aus der Evolution der Computerkriminalität von einem Forschungsgebiet der Strafrechtswissenschaft und der Kriminologie zu einem europäischen Rechtsbegriff mit Wirkungen für das unionale Primär- und Sekundärrecht sowie das mitgliedstaatliche Straf- und Verfassungsrecht. Als Computerkriminalität ist mithin nur noch ein enger Bereich von Straftaten zu bezeichnen, der die spezifischen Gefahren

---

[292] Gleichwohl wird man wohl davon ausgehen dürfen, dass die mitgliedstaatlichen Verfassungsgerichte durch ihre jeweiligen Urteile bzw. angedrohte zukünftige Beschlüsse einen signifikanten Anteil am Auslegungsprozess auf Unionsebene zeichnen. Daran lässt sich freilich der Verfassungsgerichtsdialog als Bestandteil des europäischen Rechtsfindungsprozesses erkennen.

von Computer(systeme)n aufgreift. Diese liegen unter anderem in der Geschwindigkeit von Vorgängen, der möglichen Verschiedenheit von Handlungs- und Erfolgsort sowie automatisierten Verfahren unter Ausnutzung von Netzwerkstrukturen im Allgemeinen und dem Internet im Speziellen.

Straftaten aus dem Gebiet der Angriffe auf computergestützte Systeme gehörten bei diesem Verständnis mithin zur Computerkriminalität. Klassische Delikte, inhaltsbezogene Delikte und gegen das Urheberrecht gerichtete Delikte hingegen können den hier genannten Anforderungen nicht gerecht werden. Sie sind mit dem Bereich der Computerkriminalität nur dem Namen nach vereinbar, wenn man lediglich auf eine computergestützte Begehung abstellt. Spezifische Gefahren durch die Verwendung von Computer(systeme)n entstehen aber nicht bereits durch automatisierte Abläufe oder das Auseinanderfallen von Handlungs- und Erfolgsort im Rahmen einer singulären Betrachtung. Vielmehr ist eine Kombination der genannten Bausteine notwendig, um eine tatsächlich genuine Gefährdung durch Computersysteme festzustellen. Das ist regelmäßig der Fall, wenn verschiedene computergestützte Netzwerke miteinander kommunizieren.

Die Validität einer solchen Begrenzung, die im Übrigen etwas weiter und offener ist als der Begriff der *Computerkriminalität im engeren Sinne*,[293] lässt sich mit verschiedenen Argumenten stützen. Erstens hat sich die Europäische Union bislang mit dem Schutz von Informationssystemen vor digitalen Angriffen lediglich in diesem engen Bereich betätigt, was zumindest auf eine entsprechende Priorisierung, wenn nicht gar auf ein tatsächliches begrenzendes Verständnis der Computerkriminalität hindeutet. Zweitens liegt nur dann ein abgrenzbarer Deliktsbereich vor, der nicht alleinig zur Beschreibung eines Tatwerkzeugs dient und dabei weite Teile anderer Kriminalitätsfelder ebenfalls umfasst. Drittens ist die Gefährlichkeit und damit die hauptsächliche europäische Harmonisierungsrechtfertigung der Computerkriminalität nicht auf die bloße Existenz und Verwendung eines Computers zurückzuführen, sondern ergibt sich maßgeblich aus einer Vernetzung mehrerer Computer(netzwerke). Erst dadurch wird die Basis von europäischen Rechtsangleichungen im materiellen Strafrecht, nämlich die grenzüberscheitende Dimension, relevant und erfordert eine Bekämpfung auf gemeinsamer europäischer Grundlage. Und schließlich, viertens, nimmt eine solche Auslegung des Begriffs der Computerkriminalität die gesamte Begriffsdebatte auf und trägt dem Umstand Rechnung, dass trotz des Begriffs der Computerkriminalität in Art. 83 Abs. 1 UAbs. 2 AEUV in offiziellen Mitteilungen der Europäischen Kommission zu geplanten Politiken auf

[293] Zum Begriff siehe *Piazena*, Kommunikationsmöglichkeiten des Internets, S. 112 ff. und bereits oben, Kap. 2 § 4 A.

diesem Gebiet, wie selbstverständlich, vor allem die Begriffe Internetkriminalität und Cyberkriminalität verwendet werden. Durch die Benutzung jener Begriffe wird wiederum der Netzwerkaspekt, und damit das Zusammenwirken von Computer(systeme)n betont und die mit diesem verbundene Gefährlichkeit zum Anlass für eine gemeinsame Bekämpfung auf europäischer Ebene genommen.

Letztlich ist es daher an der Zeit, den aus den Anfängen der Informatik stammenden Begriff der Computerkriminalität mitsamt seiner phänomenologisch geprägten und auf die ursprüngliche Neuartigkeit informatischer Instrumente zurückgehenden Weite zu erneuern. Mindestens hinsichtlich der Harmonisierungskompetenz des Art. 83 Abs. 1 UAbs. 2 AEUV ist dies nicht nur kriminologisch sinnvoll, sondern insbesondere unionsrechtlich geboten. Ansonsten droht unter Berücksichtigung der fortschreitenden Technisierung die Entstehung eines Kriminalitätsbereichs mit Auffangwirkung oder eine strafrechtskompetenzrechtliche Generalklausel.

Der Begriff der Computerkriminalität des Art. 83 Abs. 1 UAbs. 2 AEUV wird von den gängigen Definitionen zu weit gefasst. Er öffnet Kriminalitäts(unter)bereiche für EU-Harmonisierungsbestrebungen, die weder einer solchen bedürfen, noch eine solche rechtmäßig begründen können. Ein netzwerkspezifischer Computerkriminalitätsbegriff berücksichtigt hingegen sowohl die bereits genannten spezifischen Gefahren digitaler Technologien als auch die unionsrechtlichen Anforderungen an die Kompetenzbegründung zur EU-Strafrechtsharmonisierung. Wie die vorgenommene Untersuchung gezeigt hat, ist Computerkriminalität, zumindest für den Rechtsbegriff des Art. 83 Abs. 1 UAbs. 2 AEUV, daher folgendermaßen zu definieren:

Computerkriminalität im Sinne des Art. 83 Abs. 1 UAbs. 2 AEUV liegt vor, *wenn sowohl das Angriffsmittel als auch das Angriffsziel Daten, Computer oder Computernetzwerke sind.* Nach der hier vertretenen Ansicht ist der Computerkriminalitätsbegriff des Art. 83 Abs. 1 UAbs. 2 AEUV mithin gewissermaßen *netzwerkspezifisch* im Gegensatz zu *werkzeugbasierend* zu verstehen.

III. Konsequenzen eines netzwerkspezifischen Begriffsverständnisses

Bevor im folgenden Kapitel die bisherigen computerstrafrechtlichen EU-Rechtsakte detailliert untersucht und insbesondere auch hinsichtlich ihrer Vereinbarkeit mit dem hier entwickelten und vertretenen netzwerkspezifischen Begriff der Computerkriminalität bewertet werden,[294] ist zunächst eine übergeordnete Betrachtung der Auswirkungen eines solchen Begriffsverständnisses angezeigt.

---

294 Siehe unten, Kap. 3 § 9 D.; Kap. 3 § 10 B.; Kap. 3 § 11 D.

Grundbedingung der EU-Kompetenz zur Harmonisierung des materiellen Strafrechts mithilfe von Art. 83 Abs. 1 AEUV ist ein unionsweiter Konsens über die Strafwürdigkeit und Mindeststrafbarkeit im Bereich bestimmter Kriminalitätsbereiche. Dem Primärrecht folgend müssen diese Bereiche zudem besonders schwere und grenzüberschreitende Kriminalitätserscheinungen umfassen. Weshalb eine am Tatwerkzeug Computer anknüpfende Definition des Kriminalitätsbereichs nicht trägt, ist bereits ausführlich begründet worden. Gleichzeitig ist jedoch ebenfalls von entscheidender Bedeutung, dass eine netzwerkspezifische Bestimmung der Computerkriminalität auch tatsächlich die relevanten kriminellen Verhaltensweisen erfasst. Den Kernbereich der netzwerkspezifischen Computerkriminalität nehmen dabei grundsätzlich die sog. CIA-Delikte[295] ein. Straftaten gegen die Vertraulichkeit, Integrität und Verfügbarkeit von Computer(systeme)n und Daten sind erstens von keinem anderen Kriminalitätsbereich erfasst, können zweitens durch globale Netzstrukturen nicht nur regelmäßig transnational, sondern vor allem auch massenhaft ohne merklichen Mehraufwand verwirklicht werden und stellen schließlich drittens Straftaten dar, die ganzheitlich und nicht lediglich hinsichtlich der Tatmodalitäten auf Computer(systeme) angewiesen sind.

Beispielsweise werden über das Internet massenhaft Daten in fremden Computer(systeme)n verändert oder blockiert, indem Schadprogramme o. ä. als Tatmittel herhalten. Ebenfalls können ganze Informationsinfrastrukturen durch netzwerkspezifische Angriffe lahmgelegt oder manipuliert werden.[296] *Auch die Fernsteuerung (und ggf. die Nutzung der Rechenleistung) fremder Computer(systeme) lässt sich problemlos unter den netzwerkspezifischen Computerkriminalitätsbegriff subsumieren.*

Im Unterschied zum bereits benannten Begriff der Computerkriminalität i. e. S.[297] erfasst die netzwerkspezifische Computerkriminalität analoge Angriffe auf Daten und Computer(systeme) nicht, sondern definiert noch einmal enger. Dazu kann insbesondere auf die Vorarbeiten *Piazenas* zur Differenzierung zwischen Computerkriminalität und Internetkriminalität zurückgegriffen werden,[298] um diese durch den Aspekt der Netzwerkspezifität zu ergänzen. Während *Piazena* für die Computerkriminalität i. e. S. einen Datenaustausch nachvollziehbarerweise nicht für erforderlich hält und unter den Begriff der Internetkriminalität letztlich sämtliche mithilfe des Internets begangene Straftaten

---

295 Siehe bereits oben, Kap. 2 § 5 A.
296 Siehe dazu weiterführend unten, Kap. 4 § 13.
297 Siehe oben, Kap. 2 § 4 A.
298 *Piazena*, Kommunikationsmöglichkeiten des Internets, S. 112 ff.

subsumiert,[299] erfordert der hier vertretene netzwerkspezifische Computerkriminalitätsbegriff im Ergebnis die Kumulation der jeweiligen von *Piazena* benannten Voraussetzungen.

Das Ausspähen (§ 202a StGB), Abfangen (§ 202b StGB), Verändern (§ 303a StGB) und Sabotieren (§ 303b StGB) von Daten ist selbstverständlich auch im Zeitalter globaler Vernetzungsstrukturen weiterhin als ortsgebundene Schädigungshandlung mit analoger Eingabe von Informationen in einen Computer oder in ein Computersystem denkbar. Die Notwendigkeit einer diesbezüglichen materiellen Strafrechtsharmonisierung liegt hingegen in der Begehungsweise unter Ausnutzung kleiner und großer Netzwerke, da dann oftmals unkontrolliert territoriale Grenzen überschritten und damit unterschiedliche strafrechtliche Souveränitätsbereiche berührt werden.

Die Netzwerkspizifität als Voraussetzung der Staftaten des Bereichs der Computerkriminalität i. S. d. Art. 83 Abs. 1 UAbs. 2 AEUV schränkt die Harmonisierungskompetenz der Europäischen Union insoweit gegenüber einer phänomenologischen Begriffsdefinition erheblich ein. Erstens bedarf der schmale Bereich analog begangener Delikte gegen Daten und Computer, wie gezeigt,[300] aufgrund der regelmäßig fehlenden transnationalen Wirkungsweise keiner Harmonisierung. Zweitens fallen klassische Delikte (z. B. Erpressung per E-Mail), inhaltsbezogenen Delikte (z. B. Verbreitung verbotener Inhalte) und Urheberrechtsdelikte trotz eines etwaigen Computer(system)s als Tatwerkzeug richtigerweise aus der Definition heraus, da ihr rechtsethischer Unwertcharakter nicht im Missbrauch eines Computer(system)s, sondern vielmehr in der zugrunde liegenden Rechtsgutsschädigung besteht.[301]

E. Zwischenergebnis und Zusammenfassung

Die ersten Teile der Dissertation verstanden sich einerseits als Einkreisung der materiell-rechtlichen Aspekte eines transnationalen Computerstrafrechts durch

[299] *Piazena*, Kommunikationsmöglichkeiten des Internets, S. 112 ff., geht grundsätzlich davon aus, dass die Computerkriminalität i. w. S. in die Computerkriminalität i. e. S. und die Internetkriminalität aufzugliedern ist. Eine Aussage zum Verständnis des Begriffs im Rahmen von Art. 83 Abs. 1 UAbs. 2 AEUV trifft er damit freilich nicht.

[300] Siehe diesbezüglich auch die Ausführungen unten, Kap. 3.

[301] Einige Bereiche, wie beispielsweise Staftaten im Zusammenhang mit Kinderpornografie, können selbstverständlich unabhängig von ihrer hier abgelehnten Zuweisung zu den Computerstraftaten unionsweit harmonisiert werden, wenn sie einem anderen in Art. 83 Abs. 1 UAbs. 2 AEUV aufgeführten Kriminalitätsfeld unterfallen. Ebenfalls ist die zusätzliche Aufnahme weiterer Kriminalitätsbereiche in den Katalog grundsätzlich nach Art. 83 Abs. 1 UAbs. 3 S. 1 AEUV möglich; siehe dazu auch unten, Kap. 3 § 10 B.

Darstellung der Rechtsquellen, der verschiedenen Harmonisierungsarten und durch Eingrenzung des Untersuchungsbereichs auf den europäischen Rechtsraum. Andererseits ist der Begriff der Computerkriminalität unter historischen, technischen und rechtlichen Gesichtspunkten in sein begriffliches Umfeld eingeordnet sowie auf seine Tauglichkeit als Harmonisierungsgrundlage überprüft worden. Nachdem die Notwendigkeit einer Begriffseingrenzung identifiziert worden ist, wurde zunächst die einschränkende Lesart des Bundesverfassungsgerichts in seinem Lissabon-Urteil durch Hinweis auf die anerkannten europäischen Auslegungsregeln und die Grundsätze der umfassenden Harmonisierung verworfen. Sodann ist anhand gemeinsamer Charakteristika und eines gemeinsamen Nenners ein computerstrafrechtlicher Deliktsbereich identifiziert worden, der sowohl den europäischen Harmonisierungsnotwendigkeiten und -kompetenzen gerecht wird, als auch die mitgliedstaatlichen Kooperations- und Umsetzungserfordernisse nicht über den notwendigen Bereich der gemeinsamen europäischen Bekämpfung der Computerkriminalität hinaus überdehnt.

Kapitel 3

Harmonisierungen im EU-Computerstrafrecht

Nachdem im zweiten Teil der Arbeit für eine Beschränkung des (Rechts-)Begriffs der Computerkriminalität als Harmonisierungsgrundlage des EU-Primärrechts gestritten wurde, werden in diesem dritten Teil einerseits verschiedene EU-Harmonisierungsakte mit computerstrafrechtlichen Elementen untersucht und an der Begriffsbestimmung des zweiten Teils gemessen. Andererseits wird die Richtlinie 2013/40/EU als aktuellster EU-Rechtsakt zum Computerstrafrecht einer umfassenden Rechtmäßigkeitsprüfung hinsichtlich des EU-Primärrechts unterzogen, da sie durch noch genauer herauszuarbeitende Elemente der Vorfeldkriminalisierung eine bedenkliche Instrumentalisierung des Strafrechts zur Gefahrenprävention darstellt.

Maßgebliche Untersuchungsgegenstände sind im Folgenden erstens der Rahmenbeschluss 2001/413/JI zur Bekämpfung von Betrug und Fälschung im Zusammenhang mit unbaren Zahlungsmitteln[1], zweitens die Richtlinie 2011/92/EU zur Bekämpfung des sexuellen Missbrauchs und der sexuellen Ausbeutung von Kindern[2] und drittens die Richtlinie 2013/40/EU über Angriffe auf Informationssysteme[3]. Die Dar- und Gegenüberstellung dieser verschiedenen EU-Rechtsakte zeigt einerseits das Verständnis der EU-Institutionen im Hinblick auf ein europäischen Computerstrafrecht und andererseits die Harmonisierungsauswirkungen und Umsetzungserfordernisse für das deutsche Strafrecht auf. Die Beschränkung auf gerade diese drei Rechtsakte basiert auf der allgemeinen Ansicht, dass diese die einzigen bislang in Kraft getretenen Legislativakte der EU sind, die einen materiellen computerstrafrechtlichen Bezug aufweisen.[4]

Dieser Abschnitt bildet somit eine entscheidende Verbindung zwischen dem kompetenzrechtlich sowie interpretationsmethodisch geprägten zweiten Teil

[1] Kap. 3 § 9.
[2] Kap. 3 § 10.
[3] Kap. 3 § 11.
[4] *Hilgendorf/Valerius*, Computer- und Internetstrafrecht, § 1 Rn. 108 ff.; auch *Summers*, BJCLCJ 2015, 48 (50) nennt diese drei EU-Rechtsakte im Zusammenhang mit computerstrafrechtlichen Harmonisierungen.

und dem Abschlusskapitel der Dissertation zur zukünftigen Entwicklung eines europäischen Computerstrafrechts mit „de lege ferenda Elementen“.

Einen inhaltlichen Schwerpunkt nimmt – insbesondere hinsichtlich der aktuellsten Richtlinie 2013/40/EU über Angriffe auf Informationssysteme – mit Blick auf die §§ 202a, 202b, 202c, 263a Abs. 3, 303a und 303b StGB die Auseinandersetzung mit der weitreichenden Vorverlagerung der Strafbarkeit in den Vorbereitungsbereich ein.[5] Diese mündet schließlich in eine umfassende Rechtmäßigkeitsprüfung der Richtlinie.

§ 9 Rahmenbeschluss 2001/413/JI zur Bekämpfung von Betrug und Fälschung im Zusammenhang mit unbaren Zahlungsmitteln

Von der Erwähnung in Programmen und Zielvereinbarungen abgesehen ist der Rahmenbeschluss zur Bekämpfung von Betrug und Fälschung im Zusammenhang mit unbaren Zahlungsmitteln das erste EU-Instrument mit expliziten computerstrafrechtlichen Elementen. Insbesondere Art. 3 und 4 des Rahmenbeschlusses geben den Mitgliedstaaten detaillierte Anweisungen zur Rechtsangleichung im Computerstrafrecht.

A. Exkurs: Rechtsnatur der Rahmenbeschlüsse nach Art. 34 Abs. 2 S. 2 lit. b) EUV a. F. i. V. m. Art. 31 Abs. 1 lit. e) EUV a. F.

Vor Inkrafttreten des Vertrags von Lissabon im Jahre 2009 waren die strafrechtlichen Legislativkompetenzen der Europäischen Union in Art. 31 Abs. 1 lit. e) EUV a. F. geregelt und damit Teil des Unionsrechts, also der sog. dritten Säule. Handlungsformen waren dabei Rahmenbeschlüsse nach Art. 34 Abs. 2 S. 2 lit. b) EUV a. F. und Übereinkommen nach Art. 34 Abs. 2 S. 2 lit. d) EUV a. F.,[6] obgleich seit der Einführung des Rahmenbeschlusses als Handlungsform lediglich jenes Instrument eingesetzt wurde.[7]

Art. 31 Abs. 1 lit. e) EUV a. F. sah „die schrittweise Annahme von Maßnahmen zur Festlegung von Mindestvorschriften über die Tatbestandsmerkmale

---

[5] Derartige Vorverlagerungstendenzen finden sich auch bereits in Vorgänger-Rahmenbeschlüssen und in der Cybercrime Convention (ETS Nr. 185), die jeweils bereits in deutsches Strafrecht umgesetzt worden sind.

[6] *Dannecker*, JURA 2006, 95 (99); *Gärditz/Gusy*, GA 2006, 225 (228 ff.); *Hecker*, Europäisches Strafrecht, Kap. 11 Rn. 9.

[7] Dies lag vor allem an der Schwerfälligkeit von Übereinkommen, was insbesondere auf die zwingend notwendige Ratifikation aller Mitgliedstaaten zurückzuführen ist; vgl. dazu *Dorra*, Legislativkompetenzen, S. 58 ff. m. w. N.

strafbarer Handlungen und die Strafen in den Bereichen organisierte Kriminalität, Terrorismus und illegaler Drogenhandel" vor. Der Bereich der Computerkriminalität war zum damaligen Zeitpunkt mithin nicht von der EU-Harmonisierungskompetenz erfasst.[8] Aus kompetenzrechtlicher Perspektive bestand darüber hinaus bei zwei wesentlichen Punkten Unklarheit.

Erstens war fraglich, ob die strafrechtlichen Kompetenzen über den eigentlich klaren Wortlaut des Art. 31 Abs. 1 lit. e) EUV a. F. hinaus unter Verweis auf die Ziele des Art. 29 EUV a. F. erweitert werden könnten. Jener nennt nämlich weitere Kriminalitätsbereiche, die ein gemeinsames Vorgehen im Rahmen der dritten Säule erfordern. Teilweise wurde davon ausgegangen, dass einzig Art. 31 Abs. 1 lit. e) EUV a. F. die tatsächliche Kompetenz im Rahmen der PJZS darstellte und daher die Harmonisierungskompetenz der EU im materiellen Strafrecht auf die oben genannten Kriminalitätsbereiche beschränkt war.[9] Die herrschende Ansicht und insbesondere auch die Unionspraxis hielt hingegen nicht nur die in Art. 31 Abs. 1 lit. e) EUV a. F. explizit genannten Kriminalitätsfelder (organisierte Kriminalität, Terrorismus und illegaler Drogenhandel) für harmonisierungsfähig, sondern zog auch die zusätzlichen Zielbestimmungen des Art. 29 EUV a. F., namentlich die Bereiche Menschenhandel und Straftaten gegenüber Kindern, illegaler Waffenhandel, Bestechung und Bestechlichkeit sowie Betrug, bei der Kompetenzbegründung heran.[10] Beide Artikel des EUV a. F. sind mittlerweile in Art. 83 AEUV aufgegangen. Dieser umgeht derartige Auslegungsschwierigkeiten durch die gleichrangige und zunächst[11] abschließende Aufzählung der bereits im EUV a. F. angelegten Kriminalitätsbereiche.

Zweitens führte die Verschiedenartigkeit von Gemeinschafts- und Unionsrecht dazu, dass eine Zeit lang Richtlinien und Verordnungen zu einem Sachbereich auf das Gemeinschaftsrecht gestützt wurden, während die EU deren strafrechtliche Aspekte jeweils als Rahmenbeschlüsse auf Grundlage des Unionsrechts ausgestaltete.

---

[8] Der Entwurf des EU-Verfassungsvertrags sah die Kompetenz zur Bekämpfung von Computerkriminalität dann allerdings in Art. III-271 VerfEU vor. Auf diesem Artikel-Entwurf basiert letztlich auch der heutige Art. 83 AEUV.

[9] Siehe u. a. *Calliess*, ZEuS 2008, 3 (12 f.); so auch damals noch *Nemitz*, in: Lenz/Borchardt (Hrsg.), 4. Aufl., Art. 31 EUV 18; jetzt aber i. S. d. h. A. zur damaligen Rechtslage *Zerdick*, in: Lenz/Borchardt (Hrsg.), Art. 83 AEUV Rn. 1.

[10] Siehe insb. *Heger*, ZIS 2009, 406 (412) und *ders.*, Umweltstrafrecht, S. 140 ff., der im Ergebnis zwar die h. A. akzeptiert, im Hinblick auf den Wortlaut allerdings skeptisch bleibt; auch *Satzger*, in: Streinz (Hrsg.), Art. 83 AEUV Rn. 11; *Vogel/Eisele*, in: Grabitz/Hilf/Nettesheim (Hrsg.), 57. EL Aug. 2015, Art. 83 AEUV Rn. 48.

[11] Harmonisierungskompetenzen bezüglich zusätzlicher Kriminalitätsbereiche erfordern zuerst eine Erweiterung des Kataloges gem. den Voraussetzungen des Art. 83 Abs. 1 UAbs. 3 AEUV.

Sollte nämlich einer Maßnahme aus dem Bereich der Binnenmarktkompetenz mit strafrechtlichen Mitteln zur optimalen Wirksamkeit verholfen werden, bestand die Problematik darin, dass die Kompetenz zur Angleichung des Binnenmarkts in der „Vor-Lissabon-Zeit“ Teil des Gemeinschaftsrecht und daher im Wege der Richtlinien-Harmonisierung durchzuführen war. Strafrechtliche Anweisungskompetenzen hingegen waren Teil der dritten Säule und damit dem Unionsrecht zugeordnet, sodass eine Harmonisierung nur durch Rahmenbeschlüsse und Übereinkommen möglich war. Daher kam die Kommission auf die Idee, die Maßnahmen in einen „inhaltlichen“ und einen flankierenden strafrechtlichen Teil zwischen dem Gemeinschafts- und dem Unionsrecht aufzuspalten.[12]

Der EuGH hatte allerdings schon im Jahr 2005 in einer Entscheidung der Großen Kammer[13] diese Technik unterbunden, indem er zwar einerseits grundsätzlich die fehlende Kompetenz innerhalb des Gemeinschaftsrechts für strafrechtliche Harmonisierungsakte bestätigte, aber andererseits feststellte, dass dies den Gemeinschaftsgesetzgeber freilich nicht daran hindere, „Maßnahmen in Bezug auf das Strafrecht der Mitgliedstaaten zu ergreifen, die seiner Meinung nach erforderlich sind, um die volle Wirksamkeit der von ihm erlassenen Rechtsnormen zu gewährleisten, wenn die Anwendung wirksamer, verhältnismäßiger und abschreckender Sanktionen durch die nationalen Behörden eine zur Bekämpfung schwerer Beeinträchtigungen unerlässliche Maßnahme darstellt“.[14]

B. Inhalt und Reichweite des Rahmenbeschlusses 2001/413/JI

Der Rahmenbeschluss geht einerseits auf die Empfehlung Nr. 18 des Aktionsplans zur Bekämpfung der organisierten Kriminalität von Juni 1997[15] und andererseits auf Punkt 46 des Aktionsplans des Rats und der Kommission zur bestmöglichen Umsetzung der Bestimmungen des Amsterdamer Vertrags von Dezember 1998[16] zurück. Er bildet nach den Erwägungsgründen 4 bis 6 den materiell-rechtlichen Baustein einer europäischen Strafrechtspolitik zur Be-

---

[12] Siehe dazu fortführend und die Entwicklungen zwischen Prä- und Post-Lissabon-Zeit einordnend *Nuotio*, in: Dubber/Hörnle (Hrsg.), Criminal Law, S. 1115 (1123 f.).

[13] EuGH, Rs. C-176/03, Slg. 2005 I-07879, Rn. 38 ff. – *Umweltschutz*.

[14] EuGH, Rs. C-176/03, Slg. 2005 I-07879, Rn. 89 – *Umweltschutz*.

[15] Aktionsplan zur Bekämpfung der Organisierten Kriminalität, ABl. C 251 v. 15.8.1997, S. 1 und 12.

[16] Aktionsplan des Rats und der Kommission zur bestmöglichen Umsetzung der Bestimmungen des Amsterdamer Vertrags über den Aufbau eines Raums der Freiheit, der Sicherheit und des Rechts, ABl. C 19 v. 23.1.1999, S. 1 und 13.

kämpfung des Betrugs im transnationalen Zahlungsverkehr. Eine unmittelbare Kompetenz zur computerstrafrechtlichen Harmonisierung bestand bei Inkrafttreten des Rahmenbeschlusses zwar, wie bereits gezeigt, nicht. Kompetenzrechtliche Einwände wurden seinerzeit dennoch nicht erhoben, da die Harmonisierungskompetenz aus der Zuordnung des Rahmenbeschlusses zur Betrugsbekämpfung hergeleitet wurde.

I. Aufbau und Erwägungsgründe

Inhaltlich ist der Rahmenbeschluss dreigeteilt. Zunächst werden Begriffsbestimmungen geliefert, bevor drei Gruppen von Straftaten als Harmonisierungsobjekte aufgeführt und deren Begehungs- sowie Strafmodalitäten festgelegt werden. Abschließend folgen Regelungen zur internationalen Zusammenarbeit.

Grundlage dieses Rahmenbeschlusses bildet die offensichtliche Transnationalität von unbarem Zahlungsverkehr, der durch die Körperlosigkeit von Zahlungsabwicklungen besonders anfällig für kriminelle Handlungen ist. Nicht nur durch die Einführung einer europäischen Gemeinschaftswährung hätten sich grenzübergreifende Zahlungsströme vervielfacht und böten neue Angriffsflächen.[17] Insbesondere den von der organisierten Kriminalität ausgehenden Gefahren in diesem Bereich sollte ein angeglichenes formelles und materielles Strafrecht gegenübergestellt werden.

II. Maßgeblicher Inhalt

Zwar legt der Begriff des unbaren Zahlungsverkehrs eine computergestützte Begehungsform durchaus nahe, jedoch sind auch klassische, „analog begangene" Delikte von dem Rahmenbeschluss erfasst. Insbesondere der Diebstahl und die Fälschung von Kreditkarten, Euroscheckkarten, anderen von Finanzinstituten herausgegebenen Karten, Reiseschecks, Euroschecks, anderen Schecks und Wechseln ist durch die Mitgliedstaaten nach Art. 2 des Rahmenbeschlusses unter Strafe zu stellen.

Die Art. 3 und 4 konzentrieren sich auf die computerstrafrechtliche Dimension. Während Art. 3 den klassischen Computerbetrug beschreibt, dehnt Art. 4 die strafrechtliche Relevanz des Verhaltens auf Vorbereitungshandlungen aus, wenn diese zur Begehung von Straftaten im Sinne des Rahmenbeschlusses besonders geeignet sind.[18]

---

[17] Rahmenbeschluss 2001/413/JI, Erwägungsgründe 3 ff.

[18] Siehe insgesamt auch *Hecker*, Europäisches Strafrecht, Kap. 11 Rn. 80 ff.

III. Umsetzung in deutsches Strafrecht

Die Vorgaben des Rahmenbeschlusses waren größtenteils bereits durch verschiedene Regelungen im deutschen Strafrecht erfüllt. Notwendige Anpassungen wurden schließlich durch das 35. Strafrechtsänderungsgesetz[19] vorgenommen.

Der Computerbetrug nach § 263a StGB war aus systematischer Perspektive besonders stark von den Änderungen betroffen. Er wurde um einen Absatz 3 erweitert, der nunmehr das Herstellen, sich oder einem anderen Verschaffen, Feilhalten, Verwahren und Überlassen von bestimmten Computerprogrammen unter Strafe stellt.[20]

C. Kritische Auseinandersetzung

Trotz der weithin anerkannten Notwendigkeit, Strafbarkeitsbereiche mit transnationalen Begehungsmodalitäten EU-weit zu harmonisieren, sind die einzelnen Rechtsakte oftmals sehr grundlegender Kritik ausgesetzt. Zumeist wird bereits der Ansatzpunkt einer europäischen Strafrechtsharmonisierung kritisiert und dabei insbesondere bemängelt, dass die Grundprinzipien des materiellen Strafrechts bei EU-Rechtsakten nicht ausreichend berücksichtigt und daher auch die Auswirkungen der Harmonisierungsakte auf jene nicht hinreichend begründet werden. Europaweit seien das Erfordernis eines legitimen Schutzziels, das *Ultima-Ratio*-Prinzip, der Schuldgrundsatz, das Gesetzmäßigkeitsprinzip, das Subsidiaritätsprinzip und das Kohärenzprinzip Leitaspekte eines rechtmäßigen Einsatzes des materiellen Strafrechts und hätten daher im Sinne einer strafrechtlichen *good governance* Berücksichtigung zu finden, wenn der Unionsgesetzgeber durch Richtlinien Einfluss auf nationales Strafrecht ausübt.[21]

Hinsichtlich des Rahmenbeschlusses 2001/413/JI wird vor allem auf die umfangreichen Vorverlagerungstendenzen des Art. 4 hingewiesen und bemängelt, dass diese Strafbarkeitsausweitung zumindest einer eingehenden Begründung dahingehend bedurft hätte, weshalb bei einem solch geringen Gefährdungspotenzial bereits der Einsatz des materiellen Strafrechts gerechtfertigt sein soll.[22]

---

[19] Fünfunddreißigstes Strafrechtsänderungsgesetz zur Umsetzung des Rahmenbeschlusses des Rates der Europäischen Union v. 28.5.2001 zur Bekämpfung von Betrug und Fälschung im Zusammenhang mit unbaren Zahlungsmitteln (35. StrÄndG), BGBl. I 2001, S. 2838.

[20] Einen Gesamtüberblick zur Umsetzung des Rahmenbeschlusses in deutsches Recht bietet *Husemann*, NJW 2004, 104 ff.

[21] *Asp u. a.* (Manifest Kriminalpolitik), ZIS 2009, 697 ff.

[22] *Asp u. a.* (Manifest Kriminalpolitik), ZIS 2009, 697 (701).

D. Subsumtion unter den Begriff der Computerkriminalität des Art. 83 AEUV

Als Rechtsakt aus der Vor-Lissabon-Zeit hängt die Rechtmäßigkeit des Rahmenbeschlusses 2001/413/JI selbstverständlich nicht von einem Vorliegen der Voraussetzungen des Art. 83 Abs. 1 AEUV ab. Die Vereinbarkeit mit der damaligen Rechtslage wird darüber hinaus regelmäßig nicht infrage gestellt, da eine Kompetenz über den Kriminalitätsbereich der Betrugsbekämpfung gem. Art. 31 Abs. 1 lit. e) EUV a. F. i. V. m. Art. 29 EUV a. F. angenommen wird.

Dass hier dennoch eine Subsumtion vorgenommen wird, ist der Tatsache geschuldet, dass der Rahmenbeschluss selbst explizit die Harmonisierung von Computerstraftaten aufführt. Darüber hinaus ist er auch in der Literatur[23] als computerstrafrechtliches EU-Instrument aufgenommen worden und steht daher in der Tradition aktueller Rechtsangleichungen im Computerstrafrecht. Mehr als einer Überprüfung der Rechtmäßigkeit dient dieser Abschnitt somit der praktischen Anwendung des im Rahmen dieser Arbeit entwickelten und vertretenen Begriffs der Computerkriminalität.

I. Computerstrafrechtlicher Netzwerkaspekt

Jener oben in Kap. 2 § 8 D. II. entwickelte Begriff der Computerkriminalität umfasst Straftaten, deren Angriffsmittel *und* -ziele Computer oder Computernetzwerke sind. Wesentliches Begriffsmerkmal ist somit der Netzwerkaspekt im Rahmen der Straftat. Die Eingabe von Daten in einen Computer, ohne dass dieser durch das Internet oder ein Intranet mit weiteren Computersystemen verbunden wäre, kann daher nicht als Computerkriminalität i. S. d. Art. 83 Abs. 1 UAbs. 2 AEUV bezeichnet werden. Auch die Verwendung von Computer(netzwerke)n als Tatwerkzeuge, ohne dass gleichzeitig computerbezogene Rechtsgüter geschädigt bzw. bedroht würden, unterfällt nicht dem hier vertretenen Begriff der Computerkriminalität. Art. 3 des Rahmenbeschlusses 2001/413/JI bezeichnet etwa die Ausführung oder Veranlassung einer Übertragung von Geld durch unrechtmäßige Eingabe, Veränderung, Löschung oder Unterdrückung von Computerdaten, oder unrechtmäßiges Eingreifen in den Ablauf eines Computerprogramms oder den Betrieb eines Computersystems als Computerstraftaten.

Typischer Anwendungsfall im deutschen Strafrecht ist der Computerbetrug nach § 263a Abs. 1 StGB. Zwar handelt es sich bei diesem vor allem um eine Reaktion auf den Umstand, dass klassische Straftaten wie Diebstahl und Betrug

---

[23] Siehe beispielsweise *Reindl-Krauskopf*, ZaöRV 74 (2014), 563 (566); *Sieber*, in: ders./ Satzger/von Heintschel-Heinegg (Hrsg.), Europäisches Strafrecht, § 24 Rn. 19.

bei Nutzung technischer Tatmittel nicht ohne Weiteres einschlägig sind, sodass der Netzwerkaspekt nicht zwingend relevant wird. Beim klassischen Fall des Computerbetrugs, dem Missbrauch einer fremden ec-Karte am Geldautomaten, ist ein solcher Netzwerkaspekt i. S. d. vorgeschlagenen Definition regelmäßig nicht auf den ersten Blick gegeben. Man könnte nun grundsätzlich annehmen, dass eigentlich die Betrugsbekämpfung im Zentrum eines zu koordinierenden formellen und materiellen Strafrechts steht und dabei die computergestützte Begehungsweise lediglich ein quasi austauschbares Tatwerkzeug beschreibt. Für diese Sichtweise spräche auch die bereits erwähnte fehlende Kompetenz zur Harmonisierung der Computerkriminalität zum Zeitpunkt des Inkrafttretens des Rahmenbeschlusses. Allerdings spielen insbesondere auch Fälle mit manipulativem Vorgehen mithilfe eines Computer(system)s gegenüber einem anderen eine maßgebliche Rolle. Schließlich sind zwischen verschiedenen Kriminalitätsbereichen durchaus auch Überschneidungen möglich. Neben der Zuordnung zum Kriminalitätsbereich des Betrugs ist daher auch gleichzeitig die Einschlägigkeit des Computerstrafrechts denkbar.

Das Beispiel des ec-Kartenmissbrauchs am Geldautomaten weist nämlich dennoch zumeist netzwerkspezifische Aspekte auf. Durch den Bedienenden werden Datenverarbeitungsprozesse in Gang gesetzt, die regelmäßig mehrere Compute(netzwerke) betreffen und zusätzlich die klassischen Merkmale von Computerstraftaten i. e. S. erfüllen. Die Datenflüsse und involvierten Netzwerke sind dabei oftmals nicht auf den nationalen Raum beschränkt und beschränkbar, sodass auch eine grenzüberschreitende Dimension regelmäßig besteht. Zusätzlich betrifft das kriminelle Vorgehen des Straftäters auch nicht ausschließlich das Schutzgut des Betrugstatbestands, also das Vermögen des Opfers. Stattdessen manipuliert er in vielen Fällen auch ein Computersystem bzw. -netzwerk und beeinträchtigt damit die durch das Computerstrafrecht geschützten Rechtsgüter[24] zumindest mittelbar.[25]

Daher ist zumindest typischerweise eine computergestützte Netzwerkkriminalität gegeben, die in einer sich stetig enger vernetzenden Welt auch eine zunehmend grenzüberschreitende Dimension aufweist. Die computerstrafrechtlichen Elemente des Rahmenbeschlusses werden mithin auch vom Rechtsbegriff der Computerkriminalität des Art. 83 Abs. 1 UAbs. 2 AEUV umfasst.

---

[24] Ohne die umfangreiche Diskussion zum Rechtsgut des Computerstrafrechts an dieser Stelle zu eröffnen, wird im Folgenden von Vertraulichkeit, Integrität und Verfügbarkeit von Daten und Computersystemen als rechtlich schützenswertes Gut ausgegangen. Eine weitere Vertiefung bietet *Hsu*, in: Zöller/Sinn (Hrsg.), Strafrecht ohne Grenzen, S. 113 (116 ff.).

[25] Nach ganz h. M. schützt § 263a StGB unmittelbar nur das Rechtsgut Vermögen und computerstrafrechtliche Rechtsgüter lediglich im Rahmen eines Schutzreflexes oder mittelbar; siehe statt vieler: *Kindhäuser*, in: NK-StGB Bd. 3, 4. Aufl. 2013, § 263a Rn 2.

II. Vorbereitungshandlungen als Bestandteil eines Kriminalitätsbereichs

Bei Betrachtung von Art. 4 des Rahmenbeschlusses 2001/413/JI, der bereits das betrügerische Anfertigen, Annehmen, Sichverschaffen, Verkaufen, Weitergeben an eine andere Person oder Besitzen von Computerprogrammen, deren Zweck die Begehung einer der in Artikel 3 beschriebenen Straftaten ist, unter Strafe zu stellen vorsieht, kommt man zum Problem der Vorverlagerung der Strafbarkeit. Aus Begriffsbestimmungs- und Subsumtionsperspektive stellt dieses Harmonisierungserfordernis freilich keine Schwierigkeit dar, denn es handelt sich lediglich um die Ausweitung der Strafbarkeit einer Handlung in den deliktischen Vorfeldbereich. Die strafrechtliche Relevanz eines solchen Verhaltens ist zwar ganz generell durchaus sehr fraglich, jedoch wird nicht zu bestreiten sein, dass es, wenn man die Vorverlagerung der Strafbarkeit grundsätzlich anerkennt, auch in denselben Kriminalitätsbereich fällt wie die später beabsichtigte Tat, obwohl das Verhalten objektiv erst einmal neutraler Natur ist.[26]

Beispiel: Hacker H schreibt am heimischen Rechner ein Computerprogramm, das später dazu dienen soll, sich in andere Computernetzwerke „einzuhacken“. Allein das Schreiben des Programms weist somit keinen Netzwerkbezug auf, da zum Schreiben des Programms keine Internet- oder anderweitige Netzwerkanbindung notwendig ist.

Das Verhalten des H ist somit zunächst nicht unter den netzwerkspezifischen Computerkriminalitätsbegriff zu subsumieren. Berücksichtigt man aber die Zielsetzung, ist dies dennoch der Fall, da das geschriebene Programm nur dann Sinn ergibt, wenn H es später für die Zwecke der netzwerkspezifischen Computerkriminalität einsetzt. Das Verhalten des H dient somit, bei Einbeziehung der subjektiven Verhaltenskomponente, ausschließlich der Ermöglichung einer später zu begehenden Straftat, die der netzwerkspezifischen Computerkriminalität zuzurechnen wäre.

Denkbar sind darüber hinaus sogar Fallkonstellationen, in denen die Strafbarkeit einer Vorbereitungshandlung nicht einmal den Schutz desselben Rechtsguts wie die zugehörige volldeliktische Handlung bezweckt.

Beispiel: Die wohl h. M. sieht das Rechtsgut des Versicherungsmissbrauchs nach § 265 StGB im „Allgemeininteresse an der sozialen Leistungsfähigkeit des Versicherungswesens“.[27] *Als Vorbereitung zu einem Betrug zulasten des Versicherungsunternehmens schützt § 265 StGB somit (zumindest zusätzlich) ein anderes Rechtsgut als das Volldelikt, das ausschließlich den Vermögensschutz*

---

[26] Fortführend dazu siehe Kap. 3 § 12 D. I.

[27] Statt aller: *Lackner/Kühl*, StGB, § 265 Rn. 1 m. w. N.

zum Inhalt hat.[28] *Ein Kriminalitätsbereich hingegen umfasst auch Hilfshandlungen, die nicht dasselbe Rechtsgut betreffen wie das Kerndelikt.*

Mithin ist eine Vorfeldtat regelmäßig demselben Kriminalitätsbereich zuzuordnen wie das Volldelikt, auch wenn sie selbstständig betrachtet nicht der Definition des Kriminalitätsbereichs entspricht und sogar möglicherweise (zusätzlich) andere Rechtsgüter durch ihre Kriminalisierung geschützt werden sollen.

Bezüglich der Problematik von Vorfeldkriminalisierungen im Spannungsfeld zwischen deutschem Strafrechtsverständnis und dem Strafrecht der EU sei an dieser Stelle auf die ausführliche Rechtmäßigkeitsprüfung der Richtlinie 2013/40/EU verwiesen.[29]

E. Zusammenfassung und Bewertung

Zwar behandelt der Rahmenbeschluss 2001/413/JI nur in einem kleinen Ausschnitt computerstrafrechtlichen Verhaltens, jedoch wird er von Literatur und EU-Institutionen gleichermaßen als erstes EU-Rechtsinstrument zur Harmonisierung des Computerstrafrechts eingeordnet. Die Analyse der aus computerstrafrechtlicher Perspektive relevanten Art. 3 und 4 des Rahmenbeschlusses zeigt, dass es sich tatsächlich um eine Regelung des Kernbereichs der Computerkriminalität handelt und auch bei Anlegung eines engen Maßstabs und dem Erfordernis des computerstrafrechtlichen Netzwerkaspekts der zu regulierenden Straftaten eine Kompetenz nach Art. 83 Abs. 1 UAbs. 2 AEUV bestünde, wenn eine Neufassung in Form einer Richtlinie für notwendig erachtet würde.

§ 10 Richtlinie 2011/93/EU30 zur Bekämpfung des sexuellen Missbrauchs und der sexuellen Ausbeutung von Kindern sowie der Kinderpornografie

Auf der Ebene der Vereinten Nationen waren bezüglich des Kinderschutzes einerseits die „Erklärung der Rechte des Kindes“ von 1959[31] und andererseits die „UN-Konvention über die Rechte des Kindes“ von 1989 von überragender Be-

---

[28] Sehr kritisch zu dieser Konstruktion *Duttge*, in: FS Weber (2004), S. 284 (295), Bezug nehmend auf *Schünemann*, in: Hefendehl/von Hirsch/Wohlers (Hrsg.), Rechtsgutstheorie, S. 133 (151) und *Weber*, in: FS Baumann (1999), S. 345 (354).

[29] Siehe unten, Kap. 3 § 12 D.

[30] Richtlinie 2011/93/EU, ABl. L 335 v. 17.12.2011, S. 1; Bezeichnung berichtigt durch ABl. L 18 v. 21.1.2012, S. 7.

[31] UN-Dok. A/RES/14/1386 (1959).

deutung.[32] Auch der Europarat widmet sich seit mehreren Jahrzehnten dem Schutz von Kindern vor physischen und moralischen Gefährdungen. Unter anderem die bereits mehrfach erwähnte Cybercrime Convention aus dem Jahre 2001[33] fokussierte seine Schutzrichtung auf Kinderpornografie im Internet, indem Art. 9 der Konvention Handlubngen kriminalisiert, die inhaltlich sexuell verwerflich sind und durch Computersysteme verbreitet werden.

Mittlerweile hat sich auch die Europäische Union dem Schutz der sexuellen Selbstbestimmung von Kindern angenommen,[34] wozu sie sich durch die Unterstützung der oben genannten europäischen und globalen Abkommen ohnehin bereits verpflichtet hatte.[35] Vertragspartnerin der genannten Konvention ist die EU, trotz der grundsätzlichen Möglichkeit dazu, seit Erlangung der Rechtspersönlichkeit nach Art. 47 EUV[36] bislang allerdings nicht geworden.

A. Die Richtlinie 2011/93/EU als Weiterentwickloung des Rahmenbeschlusses 2004/68/JI

Nach vorhergehenden programmatischen Absichtserklärungen[37] stellt der Rahmenbeschluss 2004/68/JI den ersten verbindlichen EU-Rechtsakt zum Kinderschutz dar. Als EU-Instrument aus der Zeit vor dem Vertrag von Lissabon stützt er sich auf Art. 29, Art. 31 Abs. 1 lit. e) und Art. 34 Abs. 2 lit. b) EUV a. F., was die oben beschriebene Problematik der abschließenden Regelungsqualität von Art. 31 Abs. 1 lit. e) EUV a. F. nochmals verdeutlicht.[38] Da spätestens durch den Lissabon-Vertrag mit Art. 83 AEUV eine ausdrückliche Kompetenznorm ge-

---

[32] Mittlerweile ist die am 2.9.1990 in Kraft getretene Konvention von 193 Staaten (Stand: 23.2.2017) ratifiziert worden und stellt damit das weltweit verbreitetste Instrument zum Schutz der Menschenrechte dar.

[33] Cybercrime Convention (ETS Nr. 185).

[34] Programmatisch wird das auch durch das Stockholmer Programm – Ein offenes und sicheres Europa im Dienste und zum Schutz der Bürger, ABl. C 115 v. 4.5.2010, S. 1 noch einmal unterstützt.

[35] Insbesondere Art. 24 GRC nimmt darauf noch einmal Bezug; ABl. C 364 v. 18.12.2000, S. 1.

[36] Weitere Einzelheiten zur Genese der Vorschrift und insbesondere auch zur Völkerrechtspersönlichkeit der Europäischen Union finden sich bei *Dörr*, in: Grabitz/Hilf/Nettesheim (Hrsg.), 57. EL Aug. 2015, Art. 47 EUV Rn. 1 ff. m. w. N.

[37] Beispiele finden sich etwa in KOM (2005) 12 endg.: Mitteilung Strategische Ziele 2005–2009. Europa 2010 – Eine Partnerschaft für die Erneuerung Europas: Wohlstand, Solidarität und Sicherheit, in der die Kommission die Rechte des Kindes als vorrangiges Anliegen bezeichnet, und in der Mitteilung der Kommission im Hinblick auf eine EU-Kinderrechtsstrategie SEC (2009) 888, SEC (2006) 889, KOM (2006) 367 final, engl.

[38] Siehe oben, Kap. 3 § 9 A.

schaffen wurde, soll diese Problematik nach altem Recht hier allerdings nicht weiter vertieft werden.[39]

Mit diesem Rahmenbeschluss wird neben der Bekämpfung der sexuellen Ausbeutung von Kindern auch die Bekämpfung der Kinderpornografie bezweckt. Dadurch trägt der Rahmenbeschluss auch insbesondere der digitalen Dimension dieses Kriminalitätsbereichs Rechnung. Der Rahmenbeschluss stuft die Kinderpornografie in Erwägungsgrund 5 als besonders schwere Form der sexuellen Ausbeutung ein und identifiziert neue Technologien und das Internet als maßgebliche Faktoren bei der Verbreitung derselben und damit auch bei der Ausweitung des Phänomens.

Die nun aktuelle Richtlinie 2011/93/EU[40] geht zurück auf Art. 82 Abs. 2 und Art. 83 Abs. 1 AEUV und ergänzt den im Grundsatz übernommenen Rahmenbeschluss durch zusätzliche Vorgaben für effiziente Strafbarkeitsvorgaben, um eine europaweite Verfolg- und Strafbarkeit in diesem Kriminalitätsbereich sicherzustellen. Vor allem inadäquate Strafverfolgungsverfahren, die zunehmend grenzüberschreitende Dimension der Delikte und die Fortentwicklung der Informationstechnologie haben laut der Begründung des Richtlinien-Vorschlags zu einer Verschärfung der Problematik geführt und damit eine Anpassungsnotwendigkeit geschaffen.[41]

I. Computerbezogene Regelungen

Dass die Europäische Union bereits wenige Jahre nach Umsetzung des Rahmenbeschlusses 2004/68/JI einen neuen Harmonisierungsakt im Sexualstrafrecht beschlossen hat, ist insbesondere auf Schutzlücken bei Begehungsformen unter Nutzung von Informations- und Kommunikationssystemen zurückzuführen. Neu eingefügt wurde daher erstens die Kontaktaufnahme zu Kindern zum Zweck des sexuellen Missbrauchs nach Art. 6 der Richtlinie 2011/93/EU, auch bekannt als sog. Grooming. Zweitens ist nach Art. 3 Abs. 2 und 3 das Veranlassen der Zeugenschaft[42] sexueller Handlungen oder sexuellen Missbrauchs unter Strafe zu stellen. Schließlich ist Art. 5 (Straftaten im Zusammenhang mit Kin-

---

[39] *Geiger*, Strafrechtsharmonisierungen, S. 198 ff., bietet dazu ausführliche Hinweise.

[40] Richtlinie 2011/93/EU, ABl. L 335/1 v. 17.12.2011.

[41] Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rats zur Bekämpfung des sexuellen Missbrauchs und der sexuellen Ausbeutung von Kindern sowie der Kinderpornografie und zur Aufhebung des Rahmenbeschlusses 2004/68/JI des Rats, KOM (2010) 94 endg., S. 3.

[42] Unter dem Veranlassen der Zeugenschaft ist zu verstehen, dass sich derjenige strafbar macht, der zu sexuellen Zwecken ein Kind mit sexuellen Handlungen oder sexuellem Missbrauch konfrontiert, auch ohne dass jenes daran aktiv teilnimmt.

derpornografie) als Regelung mit Bezug zu einer computergestützten Begehungsweise einzuordnen.[43]

II. Umsetzungserfordernisse und Abweichungsmöglichkeiten

Der Umsetzungsbedarf bezüglich computerstrafrechtlicher Elemente besteht für Deutschland an verschiedenen Stellen. Insbesondere im Bereich der kinderpornografischen Darbietungen im Rahmen von Livestreams, die mit oder ohne Zwischenspeicherung im Browser-Cache stattfinden, sind Nachbesserungen im deutschen Recht angezeigt. Beachtenswert sind außerdem die Abweichungsmöglichkeiten, die den nationalen Gesetzgebern eröffnet werden. Vor allem im Bereich der Schein- und Fiktivpornografie[44] nach Art. 5 Abs. 7 und 8 liegt es im Ermessen der Mitgliedstaaten, gegebenenfalls von einer Strafbarkeit abzusehen.

B. Subsumtion unter den netzwerkspezifischen Computerkriminalitätsbegriff

Computerkriminalität als Rechtsbegriff bezeichnet nach der hier vertretenen Auffassung netzwerkorientierte Straftaten im Zusammenhang mit dem Einsatz von Computer(systeme)n als Angriffsmittel und -ziel.[45] Ob die durch die Richtlinie 2011/93/EU zu harmonisierenden Delikte diese Voraussetzung erfüllen, ist sehr fraglich.

Der Tatbestand des Groomings nach Art. 6,[46] als für viele Strafrechtsordnungen neues Phänomen, stellt bereits einen schwierig zu fassenden Fall dar. Er nimmt zwar explizit auf die Verwendung von Informations- und Kommunikationstechnologie Bezug und stellt auch lediglich diesen Weg der Kontaktaufnah-

---

[43] Aus der Forderung der Erwägungsgründe 46 und 47 nach einer Löschung bzw. Sperrung des Zugangs von Internetseiten mit kinderpornografischem Material ergeben sich allerdings vielschichtige Problematiken im Spannungsfeld zwischen sicherheitsrechtlich, angeblich notwendiger staatlicher Zensur und verfassungsrechtlich garantierten Meinungs- und Informationsfreiheiten. Siehe dazu ausführlich *Sieber*, JZ 2009, 653 ff.

[44] Scheinpornografie in Bezug auf Kinder und Jugendliche bezeichnet die pornografische Darstellung von Personen, die lediglich ihrem Erscheinungsbild nach unter 18 Jahren alt sind. Unter dem Begriff der Fiktivpornografie versteht man hingegen die pornografische Darstellung irrealer (z. B. computeranimierter oder gezeichneter) Kinder und Jugendlicher.

[45] Vgl. oben, Kap. 2 § 8 D. II.

[46] „Ein Erwachsener, der einem Kind, das das Alter der sexuellen Mündigkeit noch nicht erreicht hat, mittels Informations- und Kommunikationstechnologie in der Absicht, eine Straftat nach Artikel 3 Absatz 4 oder Artikel 5 Absatz 6 zu begehen, ein Treffen vorschlägt, wird mit Freiheitsstrafe im Höchstmaß von mindestens einem Jahr bestraft, wenn auf diesen Vorschlag auf ein solches Treffen hinführende konkrete Handlungen gefolgt sind.“

me und -anbahnung unter Strafe,[47] was eine computerstrafrechtliche Einordnung zunächst einmal durchaus nahelegt. Die expliziten Verweise auf die Begehungsabsicht hinsichtlich einer Straftat nach Art. 3 Abs. 4 (sexueller Missbrauch von Kindern) oder Art. 5 Abs. 6 (Herstellung von Kinderpornografie) sowie weitere auf diese Taten hinführende konkrete Handlungen machen allerdings deutlich, dass nur dann eine Strafbarkeit begründet werden soll, wenn über die digitale Kontaktaufnahme hinaus weitere Voraussetzungen erfüllt sind. Die Grooming-Strafbarkeit stellt also streng genommen gar kein genuin „neues" Delikt dar, sondern weitet die Strafbarkeit des sexuellen Missbrauchs von Kindern und der Herstellung von Kinderpornografie in bestimmten Fällen (Kontaktanbahnung über Informations- und Kommunikationstechnologie *und kumulativ* auf ein solches Treffen hinführende konkrete Handlungen) auf den Bereich der Vorbereitungshandlungen aus.[48] Tatsächlich liegt somit kein Computerdelikt vor, da lediglich die strafbarkeitsbegründende Rechtsgutgefährdung in Fällen des sexuellen Missbrauchs von Kindern und der Herstellung von Kinderpornografie derartig gelockert wird, dass bereits vorgelagerte Handlungen eine Strafbarkeit festlegen, wenn sie mittels Informations- und Kommunikationstechnologien erfolgen.

Beispiel: Sollte der (EU-)Gesetzgeber auf die Idee kommen, dass bereits die Verabredung mit einem zukünftigen potenziellen Mordopfer unter Ausnutzung der Informations- und Kommunikationstechnologie unter Strafe zu stellen ist, würde dies an der Einordnung in den Kriminalitätsbereich der „Straftaten gegen das Leben" nichts ändern.

Diese Differenzierung trifft gewissermaßen den Kernbereich der hier vorgenommenen Begriffsbestimmung. Sollten allein die Begehungsmodalitäten, oder, wie in diesem Falle, bereits ein Aspekt der Begehungsmodalitäten, ausreichen, um die Betroffenheit eines Kriminalitätsbereichs nach Art. 83 Abs. 1 UAbs. 2 AEUV anzunehmen, wären einer Ausweitung der EU-Harmonisierungsbefugnisse im Bereich des materiellen Strafrechts faktisch keine Grenzen mehr gesetzt. Um eine Vorbereitungshandlung EU-weit kriminalisieren zu können, bedarf es daher einer Harmonisierungskompetenz des dem Volldelikt zugrunde liegenden Kriminalitätsbereichs.[49]

---

[47] Richtlinie 2011/93/EU, Erwägungsgrund 19 weist zusätzlich auch explizit auf die Strafwürdigkeit der Kontaktanbahnung eines Erwachsenen zu einem Kind zu sexuellen Zwecken ohne Nutzung der Informations- und Kommunikationstechnologien hin.

[48] Statt aller: *Lackner/Kühl*, StGB, § 176 Rn. 4a; *Renzikowski*, in: MüKo-StGB Bd. 3, § 176 Rn. 37.

[49] Auch *Piazena*, Kommunikationsmöglichkeiten des Internets, S. 115, macht deutlich, dass es sich etwa beim Verkaufen nicht existenter Ware im Internet weiterhin um einen Be-

Mit der oben bereits dargestellten und begründeten Auffassung, dass die volldeliktische Handlung den Kriminalitätsbereich auch für zugehörige Vorbereitungshandlungen vorgibt, ist das Grooming dem Kriminalitätsbereich des Menschenhandels und der sexuellen Ausbeutung von Frauen und Kindern zuzuordnen. Wie erwähnt, sind zwar selbstverständlich bei derartig offen gestalteten Begriffen auch Überschneidungen denkbar, wie sich schon bei der computerstrafrechtlichen Einordnung des Computerbetrugs gezeigt hat.[50] Obwohl dieser lediglich einen Spezialfall des Betrugs beschreibt, sind das Delikt und auch etwaige Vorbereitungshandlungen nicht nur dem Bereich der Vermögensdelikte, sondern eben auch der Computerkriminalität zuzurechnen. Das liegt allerdings daran, dass bei der Tatbegehung regelmäßig, zumindest mittelbar, auch selbstständige netzwerk- und computerspezifische Rechtsgutsbeeinträchtigungen oder -gefährdungen auftreten. Beim Grooming liegt der Fall jedoch anders. Computersysteme und -netzwerke werden nicht manipuliert, beschädigt oder zerstört, sondern lediglich als Kommunikationsmittel genutzt. An anderer Stelle[51] ist auf die Problematik des Tatmittels „Computer“ als alleinigem Anknüpfungspunkt für eine Harmonisierungskompetenz bereits hingewiesen worden. Die Grooming-Strafbarkeit hat mit einer netzwerkspezifischen Computerkriminalität nicht mehr gemein als etwa Drogenhandel, der mithilfe eines E-Mail-Verkehrs abgewickelt wird, sodass sich eine Harmonisierungskompetenz nicht auf diesen Kriminalitätsbereich stützen lässt.

Auch bei der zweiten Grooming-Variante nach Art. 6 Abs. 2 der Richtlinie 2011/93/EU[52] handelt es sich um ein klassisches Sexualdelikt, bei dem lediglich die Informations- und Kommunikationstechnologie als Hilfsmittel zur Tatverwirklichung eingesetzt wird. Eine Subsumtion unter den Rechtsbegriff der Computerkriminalität gelingt daher auch in diesem Fall aus o. g. Gründen nicht.

Die Strafbarkeit der Kinderpornografie nach Art. 5 wird in Teilen an moderne Begehungsformen unter Verwendung der Informations- und Kommunikationstechnologie angepasst, um sicherzustellen, dass die Strafbarkeit nicht von natio-

---

trug und damit um ein Vermögensdelikt und beim Versenden einer beleidigenden E-Mail weiterhin um ein Äußerungsdelikt handelt.

[50] Siehe bereits oben, Kap. 3 § 9 D.

[51] Vgl. oben, Kap. 2 § 8 B.

[52] „Die Mitgliedstaaten treffen die erforderlichen Maßnahmen, um sicherzustellen, dass der Versuch eines Erwachsenen, mit Mitteln der Informations- und Kommunikationstechnologie Straftaten gemäß Artikel 5 Absatz 2 und 3 [Einschub des Verfassers: Erwerb von Kinderpornografie und der bewusste Zugriff auf Kinderpornografie mittels Informations- und Kommunikationstechnologie] zu begehen, indem er Kontakt zu einem Kind, das das Alter der sexuellen Mündigkeit noch nicht erreicht hat, aufnimmt, um kinderpornografische Darstellungen dieses Kindes zu erhalten, strafbar ist.“

nalen Besonderheiten[53] abhängt, sondern die Straf- und Verfolgbarkeit auch bei Tathandlungen wie der Teilnahme an kinderpornografischen Darbietungen mittels Informations- und Kommunikationstechnologie gegeben ist.[54] Insbesondere im deutschen Strafrecht wird teilweise angenommen, dass eine Schutzlücke des „besitzlosen Konsums“ (beispielsweise beim bloßen „Surfen“ im Internet) von Kinderpornografie besteht. Die Rechtsprechung behilft sich regelmäßig damit, auf § 184b Abs. 3 S. 1 Alt. 1 StGB (Unternehmen der Verschaffung) abzustellen, wenn weder ein Herunterladen noch eine Zwischenspeicherung, sondern lediglich ein reines Betrachten des kinderpornografischen Materials erfolgte.[55] Da die Literatur dieser Hilfskonstruktion allerdings mehrheitlich skeptisch gegenübersteht,[56] ist eine Klarstellung i. S. d. Art. 5 der Richtlinie 2011/93/EU wünschenswert. Denkbar wäre insoweit etwa, auf das Erfordernis des Besitzes eines physischen Gegenstands zu verzichten.[57]

Eine Subsumtion unter den Begriff der Computerkriminalität ist allerdings auch in diesen Fällen abzulehnen. Trotz einer Erleichterung und Beschleunigung der Verfügbarkeit und Verbreitung von Kinderpornografie durch die Informations- und Kommunikationstechnologie mit ihren Computernetzwerken schützen die zugrunde liegenden Strafbarkeiten weiterhin die sexuelle Selbstbestimmung von Kindern und Jugendlichen und sind damit eindeutig dem Sexualstrafrecht zuzuordnen. Eine zusätzliche Klassifizierung als Bestandteil der Computerkriminalität schafft einerseits Inkonsistenzen und ermöglicht andererseits die extensive Kompetenzbegründung der Europäischen Union, die insbesondere im Strafrecht strikt abzulehnen ist.

Für eine Einordnung der Kinderpornografie als Bestandteil der Computerkriminalität wird etwa vorgetragen, dass erst durch die Existenz von Computernetzwerken ein globaler Markt für Kinderpornografie geschaffen worden ist.[58] Man könnte daher sagen, dass Kinderpornografie, wie sie sich heutzutage präsentiert, ohne Computernetzwerke gar nicht mehr vorstellbar und daher eine

---

[53] § 184b Abs. 3 StGB stellt den Besitz kinderpornografischer Schriften unter Strafe und wäre selbstständig somit nicht geeignet, digitale Versionen kinderpornografischen Materials zu kriminalisieren. § 11 Abs. 3 StGB erweitert den Schriftenbegriff daher auf „Datenspeicher“.

[54] Siehe dazu Art. 4 Abs. 4 und Art. 2 lit. e) Richtlinie 2013/40/EU.

[55] Vgl. OLG Hamburg, NJW 2010, 1893 (1895), damals noch bzgl. § 184b Abs. 4 S. 1 StGB a. F.

[56] *Fischer*, StGB, § 184b Rn. 34 f.; *Hörnle*, in: MüKo-StGB Bd. 3, § 184b Rn. 35.; *Popp*, ZIS 2011, 193 (196 ff.).

[57] So auch *Brodowski*, in: Lange/Bötticher (Hrsg.), Cyber-Sicherheit, S. 249 (255) m. w. N., der einen Wandel vom Sach- zum Informationsbezug vorschlägt.

[58] Beispielhaft stehen dafür die Regelungen und Erklärungen in der Cybercrime Convention (ETS Nr. 185) und der Richtlinie 2011/93/EU.

Zuordnung zu diesem Kriminalitätsbereich gerechtfertigt sei, da gewissermaßen eine grundlegende Wandlung des Straftatbestands stattgefunden habe. Auch wenn aktuell tatsächlich ein Großteil der Kinderpornografie mithilfe von Computernetzwerken verbreitet wird und auch jene erst durch diese Globalisierung zu einem flächendeckenden Problem geworden ist, kommt eine Neuverortung im Kriminalitätsbereich der Computerkriminalität nicht in Betracht. Computernetzwerke stellen eine Kommunikationsinfrastruktur dar, die für sich selbst genommen durchaus schützenswert ist. Wenn aber lediglich unter Ausnutzung dieser Infrastruktur Straftaten begangen werden, unterfallen diese nicht dem Bereich der „Infrastruktur"-Kriminalität selbst. Ein Beispiel ist der Bereich der Verkehrsdelikte. Dieser zeichnet sich dadurch aus, dass etwa die Straftaten der §§ 315b, 315c, 316, 316a StGB nach der h. M. vorwiegend den Straßenverkehr als solchen schützen.[59] Herkömmliche Straftaten, die lediglich bei Gelegenheit des Straßenverkehrs begangen werden, sind regelmäßig nicht Bestandteil der Verkehrsdelikte.[60] Auch der Umstand, dass einige Straftaten, wie etwa Zollvergehen und Menschenhandel, erst durch globale Zusammenschlüsse mehrerer Verkehrsinfrastrukturnetzwerke in großer Anzahl auftreten, macht diese nicht zu Verkehrsdelikten. Analog zu dieser Abgrenzung zwischen Delikten, die sich gegen eine Verkehrsinfrastruktur selbst richten, von solchen, die lediglich unter Nutzung jener Infrastruktur verübt werden, sind auch die Straftaten der Richtlinie 2011/93/EU nicht der Computerkriminalität zuzuordnen.

Auch systematische und teleologische Aspekte einer unionsrechtlichen Perspektive stehen einer Ausklammerung der Richtlinie 2011/93/EU aus dem Bereich der Computerkriminalität nicht entgegen. Derartige Argumente könnten beispielsweise dann überwiegen, wenn der Schutz der sexuellen Selbstbestimmung (von Kindern) im Hinblick auf Pornografiestraftaten auf EU-Ebene verhindert würde, weil der Computerkriminalitätsbereich zu eng verstanden wird. Dem Effektivitätsgrundsatz des EU-Rechts liefe eine solche begrenzende Auslegung dann zuwider. Art. 83 Abs. 1 UAbs. 2 AEUV beinhaltet allerdings einen einschlägigen Kriminalitätsbereich, sodass eine Anknüpfung der volldeliktischen Handlung an jenen möglich ist, ohne in extensiver Form und durch die Heranziehung von Begehungsmodalitäten in den Bereich der Computerkrimi-

---

[59] BGHSt 48, 119 (123); zum Streitstand siehe *Geppert*, Jura 2001, 559 (560); *Hentschel/König*, § 315b StGB Rn. 1; *Zieschang*, in: NK-StGB Bd. 3, § 315b Rn. 1; *König*, in: LK-StGB Bd. 11, § 315b Rn. 3; *Schmidt/Priebe*, BT/I, Rn. 557; *Zieschang*, in: NK-StGB Bd. 3, § 315c Rn. 5.

[60] Selbstverständlich können trotzdem mit einer Handlung sowohl Verkehrsdelikte als auch Delikte gegen die körperliche Unversehrtheit begangen werden. Steinwürfe von Autobahnbrücken (BGH NStZ-RR 2010, 373 f.) etwa begründen gleichzeitig die Strafbarkeiten des (versuchten) Mordes und des gefährlichen Eingriffs in den Straßenverkehr.

nalität vorzudringen, um eine Kompetenz zu begründen. Nach verbreiteter Auffassung stellen nämlich der sexuelle Missbrauch und die Kinderpornografie eine Untergruppe des Kriminalitätsbereichs der „sexuellen Ausbeutung von Frauen und Kindern" dar, der bereits selbstständig in Art. 83 Abs. 1 UAbs. 2 AEUV aufgeführt ist.[61]

C. Zusammenfassung und Bewertung

Eine Kompetenz zur Harmonisierung des Kinderpornografie-Strafrechts kann nach ganz überwiegender Auffassung durch den Kriminalitätsbereich „Menschenhandel und sexuelle Ausbeutung von Frauen und Kindern" begründet werden. Der Kriminalitätsbereich der Computerkriminalität in seiner hier vertretenen Ausprägung ist indes nicht einschlägig, sodass eine Einordnung der Richtlinie 2011/93/EU als computerstrafrechtliches EU-Instrument abzulehnen ist. Dem Vorwurf des „Schattenboxens", da schließlich jedenfalls eine Kompetenz aus Art. 83 Abs. 1 UAbs. 2 AEUV zur Harmonisierung der beinhalteten Straftaten besteht, kann entgegengehalten werden, dass sich die hier vertretene Auffassung selbstverständlich abstrahieren lässt. Somit zeitigt sie auch beispielsweise für die Frage der Harmonisierungsfähigkeit von Äußerungsdelikten unter Nutzung der Infrastrukturen von Computernetzwerken zukünftig Wirkung.

§ 11 Richtlinie 2013/40/EU über Angriffe auf Informationssysteme

Die Richtlinie 2012/40/EU[62] ersetzt den Rahmenbeschluss 2005/222/JI und war durch die sich beteiligenden Mitgliedstaaten bis zum 4. September 2015 umzusetzen.[63] Aufgrund von Zusatzprotokollen wirken Irland, Großbritannien und

---

[61] *Vogel/Eisele*, in: Grabitz/Hilf/Nettesheim (Hrsg.), 57. EL Aug. 2015, Art. 83 AEUV Rn. 55. Ältere Auffassungen unterschieden noch zwischen dem klassischen Sexualstrafrecht und der sexuellen Ausbeutung von Frauen und Kindern. Dabei bezogen sie sich auf die Herstellung des kompetenzrechtlichen Zusammenhangs zwischen den Begriffen „Menschenhandel" und „sexuelle Ausbeutung", sodass nur im Zusammenhang mit dem Menschenhandel stehende Sexualdelikte, wie etwa die Prostitution, erfasst waren. Nach den bislang unwidersprochenen modernen Auffassungen sind jedoch weite Teile des Sexualstrafrechts durch Art. 83 Abs. 1 UAbs. 2 AEUV harmonisierbar.

[62] Richtlinie 2013/40/EU des Europäischen Parlaments und des Rats v. 12.08.2013 über Angriffe auf Informationssysteme und zur Ersetzung des Rahmenbeschlusses 2005/222/JI des Rates, ABl. L 218 v. 14.8.2013, S. 8.

[63] Als Vor-Lissabon-Instrument stützte sich der Rahmenbeschluss 2005/222/JI noch auf

Däne-mark jeweils nur in begrenztem Umfang an den EU-Politiken zu Innerem und Justiz mit.[64] Daher sind EU-Richtlinien bezüglich des Raums der Freiheit, der Sicherheit und des Rechts für diese Mitgliedstaaten auch regelmäßig nicht verbindlich.

Der EU-Gesetzgeber ging bei Erlass der Richtlinie davon aus, dass die Vorschriften des Rahmenbeschlusses weitgehend in nationales Strafrecht umgesetzt worden sind, allerdings aktuelle Entwicklungen auch Erweiterungen erfordern. Daher sind einerseits sämtliche Vorschriften des Rahmenbeschlusses auch in der Richtlinie enthalten und andererseits weitere Delikte aufgenommen worden, die vor allem auf die Bekämpfung von groß angelegten Cyberangriffen abzielen. Abgesehen von Dänemark beteiligen sich alle EU-Mitgliedstaaten an der Richtlinie, sodass der Vorgänger-Rahmenbeschluss, außer für Dänemark, lediglich hinsichtlich seiner Umsetzungsfristen noch Bedeutung behält.[65]

Dieser Abschnitt beschäftigt sich zunächst inhaltlich mit der Richtlinie,[66] bevor auf Gemeinsamkeiten und Unterschiede mit der bereits europaweit etablierten Cybercrime Convention eingegangen wird.[67] Anschließend erfolgt eine Auseinandersetzung mit der auf beide Rechtsakte zurückgehenden Vorverlagerung der Strafbarkeit in den Vorbereitungsbereich,[68] bevor abschließend den Fragen einer EU-rechtlichen Nichtigkeit der Richtlinie[69] bzw. der Möglichkeit zur Auslösung des sog. Notbremsemechanismus gem. Art. 83 Abs. 3 AEUV nachgegangen wird.[70]

Art. 29, Art. 30 Abs. 1 lit. a), Art. 31 Abs. 1 lit. e) und Art. 34 Abs. 2 lit. b) EUV a.F. Inhaltlich stellt er gewissermaßen ein Minus zur ihn ersetzenden Richtlinie dar, was aus materiell-rechtlicher Perspektive insbesondere durch das Fehlen einer Regelung zum Abfangen von Daten sichtbar wird. Weitere Hinweise zum Diskussionsstand vor der Ersetzung des Rahmenbeschlusses durch die Richtlinie finden sich bei *de Hert/Gonzáles Fuster/Koops*, Revue Internationale de Droit Pénal, 77 (2006), 473 und bei *Summers u. a.*, EU Criminal Law, S. 234 ff.

[64] Protokoll (Nr. 21) über die Position des Vereinigten Königreichs und Irlands hinsichtlich des Raums der Freiheit der Sicherheit und des Rechts, ABl. C 115 v. 9.5.2008, S. 295 und Protokoll (Nr. 22) über die Position Dänemarks hinsichtlich des Raums der Freiheit der Sicherheit und des Rechts, ABl. C 115 v. 9.5.2008, S. 299.

[65] *Sieber*, in: ders./Satzger/von Heintschel-Heinegg (Hrsg.), Europäisches Strafrecht, § 24 Rn. 69 ff.

[66] Kap. 3 § 11 A.

[67] Kap. 3 § 11 E.

[68] Kap. 3 § 12.

[69] Kap. 3 § 12 D.

[70] Kap. 3 § 12 D. II. 2.

A. Aufbau und Erwägungsgründe

Die Richtlinie beginnt wie bereits der Rahmenbeschluss in Art. 2 mit Definitionen zu „Informationssystem“[71], „Computerdaten“[72], „juristische Person“[73] und dem Merkmal „unbefugt“[74], bevor in den Art. 3–7 auf die einzelnen zu harmonisierenden Strafvorschriften eingegangen wird. In Art. 8 und 9 werden Anstiftung, Beihilfe und Versuch geregelt beziehungsweise die im jeweiligen nationalen Strafrecht zu verankernden Strafen festgelegt. Die Art. 10 und 11 begründen einerseits die Verantwortlichkeit von juristischen Personen und statuieren andererseits die gegen jene zu verhängenden Sanktionen. Art. 13 enthält schließlich Vorgaben zum Informationsaustausch bezüglich computerstrafrechtlicher Delikte.

Nach den Erwägungsgründen dieser Richtlinie stellen Informationssysteme unverzichtbare Bestandteile des politischen, wirtschaftlichen und gesellschaftlichen Zusammenlebens dar, sodass Angriffe auf jene oftmals schwerwiegende Beeinträchtigungen nach sich ziehen können. Insbesondere wenn diese im Zusammenhang mit organisierter Kriminalität stehen, auf kritische Infrastrukturen abzielen oder politische Ziele verfolgen, sei das europäische Ziel einer sicheren Informationsgesellschaft und die Gewährleistung eines Raumes der Freiheit, der Sicherheit und des Rechts massiv gefährdet. Gegenmaßnahmen auf EU-Ebene und darüber hinaus erforderten daher zusätzlich eine internationale Koordinierung.

Vor allem der wachsenden Zahl von Cybergroßangriffen soll durch die harmonisierte Kriminalisierung bestimmter Verhaltensweisen begegnet werden.

---

[71] „Informationssystem [bezeichnet] eine Vorrichtung oder eine Gruppe miteinander verbundener oder zusammenhängender Vorrichtungen, die einzeln oder zu mehreren auf der Grundlage eines Programms die automatische Verarbeitung von Computerdaten durchführen, sowie die von ihr oder ihnen zum Zwecke des Betriebs, der Nutzung, des Schutzes und der Pflege gespeicherten, verarbeiteten, abgerufenen oder übertragenen Computerdaten“; vgl. Art. 2 lit. a) Richtlinie 2013/40/EU.

[72] „Computerdaten [sind] jede Darstellung von Tatsachen, Informationen oder Konzepten in einer für die Verarbeitung in einem Informationssystem geeigneten Form, einschließlich eines Programms, das die Ausführung einer Funktion durch ein Informationssystem auslösen kann“; vgl. Art. 2 lit. b) Richtlinie 2013/40/EU.

[73] „Juristische Person [ist] jedes Rechtssubjekt, das den Status der juristischen Person nach dem anwendbaren Recht besitzt, mit Ausnahme von Staaten oder anderen Körperschaften des öffentlichen Rechts in der Ausübung hoheitlicher Rechte und von öffentlich-rechtlichen internationalen Organisationen“; vgl. Art. 2 lit. c) Richtlinie 2013/40/EU.

[74] „Unbefugt [ist] ein in dieser Richtlinie genanntes Verhalten, einschließlich Zugang, Eingriff oder Abfangen, das vom Eigentümer oder einem anderen Rechtsinhaber des Systems oder eines Teils des Systems nicht gestattet wurde oder das nach den einzelstaatlichen Rechtsvorschriften nicht zulässig ist“; vgl. Art. 2 lit. d) Richtlinie 2013/40/EU.

Im Vorfeld solcher Cybergroßangriffe werden in der Regel sog. Botnetze geschaffen, indem eine Vielzahl von Rechnern oder ganze Computersysteme, zumeist durch gezielte Infizierung mit Schadsoftware, zusammengeschlossen werden, um daraufhin diese multiplizierte Rechenleistung zu koordinierten Angriffen auszunutzen.[75] Ein maßgebliches Ziel der Richtlinie ist es daher, bereits die Herstellung solcher Botnetze EU-weit unter Strafe zu stellen. Von einer Deliktsverwirklichung wird dann ausgegangen, wenn „die Einrichtung einer ferngesteuerten Kontrolle über eine bedeutende Anzahl von Computern [erreicht ist], indem diese durch gezielte Cyberangriffe mit Schadsoftware infiziert werden".[76]

Weitere relevante Erwägungsgründe beziehen sich auf die sog. *dual-use*-Problematik,[77] die Einrichtung und Nutzung von internationalen Netzwerken sowie die Zusammenarbeit mit Privaten zum Informationsaustausch bei Sicherheitsvorfällen[78] und schließlich auf die allgemeine Verbesserung der Cybersicherheit als Präventivmaßnahme.[79]

Zusammengefasst handelt es sich bei der Richtlinie einerseits um eine Modernisierung gegenüber dem Rahmenbeschluss, da die Vorschriften insbesondere eine Reaktion auf die Gefahr von Botnetzen darstellen, indem bereits frühzeitig eine Strafbarkeit begründet und nicht der Einsatz eines solchen Botnetzes abgewartet wird.[80] Andererseits liegt in der Richtlinie auch eine Verschärfung der Kriminalisierungspflicht von Computerdelikten, was sich vor allem an den geforderten Strafrahmen des Art. 9 zeigt. Jener Art. 9 verlangt den Mitgliedstaaten nicht nur Maßnahmen mit wirksamen, verhältnismäßigen und abschreckenden Sanktionen ab, wie in weiten Teilen der Vorgänger-Rahmenbeschluss,[81] sondern gibt detaillierte und qualifizierte Erfordernisse zu Mindest-Höchststrafen vor. Insbesondere Art. 9 Abs. 4 der Richtlinie verdeutlicht

---

[75] Siehe zur Funktionsweise von Botnetzen sowie deren kriminologischer Einordnung im Spannungsfeld zwischen Mensch und Maschine *van der Wagen/Pieters*, Brit. J. Criminol. 2015, 578 (580 ff.).

[76] Richtlinie 2013/40/EU, Erwägungsgrund 5.

[77] Von der *dual-use*-Möglichkeit eines Tatwerkzeugs wird dann gesprochen, wenn es derartig beschaffen ist, dass neben der kriminellen Nutzung auch ein rechtmäßiger Einsatz in Betracht kommt. Daher ist bei solchen Tatwerkzeugen dolus directus Voraussetzung für die Strafbarkeit, vgl. Richtlinie 2013/40/EU, Erwägungsgrund 16. Eine vertiefende Auseinandersetzung mit dem computerstrafrechtlichen *dual-use*-Phänomen findet sich bei *Albrecht*, Dual-Use-Software, S. 11 ff.

[78] Richtlinie 2013/40/EU, Erwägungsgründe 22–24.

[79] Richtlinie 2013/40/EU, Erwägungsgrund 26.

[80] Richtlinie 2013/40/EU, Erwägungsgrund 5.

[81] Für Straftaten nach Art. 3 und 4 des Rahmenbeschlusses wurden auch in diesem bereits Höchststrafen von mindestens einem Jahr verlangt.

die Verschärfung durch die Vorgabe von Mindest-Höchststrafen von fünf Jahren in Fällen der Art. 4 und 5, wenn die entsprechenden Straftaten im Rahmen einer kriminellen Vereinigung begangen werden (lit. a), einen schweren Schaden verursachen (lit. b) oder gegen ein Informationssystem einer kritischen Infrastruktur verübt werden (lit. c).

B. Materiell-rechtlicher Regelungsbereich der Richtlinie

Den Kern der Richtlinie bilden die Art. 3–8 mit ihren Regelungen zu materiellen Harmonisierungserfordernissen.

I. Rechtswidriger Zugang zu Informationssystemen

Der rechtswidrige Zugang zu Informationssystemen[82] wird nicht nur in der Laiensprache oftmals auch als Hacking[83] bezeichnet. Interessant an der Formulierung des Artikels ist insbesondere, dass, anders als aktuell noch in vielen nationalen Rechtsordnungen,[84] bereits der Zugang zum Informationssystem und nicht erst der tatsächliche Zugriff auf Computerdaten zu kriminalisieren ist. Darüber hinaus ist wichtig, dass nur dann eine Kriminalisierung erforderlich ist, wenn Sicherheitsmaßnahmen beim Zugang verletzt werden, und dass leichte Fälle von einer Bestrafung ausgenommen werden können. Die Definition leichter Fälle wird den nationalstaatlichen Gesetzgebern überlassen, obgleich Erwägungsgrund 11 darauf hindeutet, dass vor allem die Geringfügigkeit des verursachten Schadens oder der Gefahr maßgeblich sein sollte.

---

[82] Art. 3 der Richtlinie 2013/40/EU: „Die Mitgliedstaaten treffen die erforderlichen Maßnahmen, um sicherzustellen, dass der vorsätzliche unbefugte Zugang zu einem Informationssystem als Ganzem oder zu einem Teil davon, wenn dieser Zugang durch eine Verletzung von Sicherheitsmaßnahmen erfolgt, zumindest dann unter Strafe gestellt wird, wenn kein leichter Fall vorliegt.“

[83] Unter Hacking werden Handlungen subsumiert, die darauf abzielen, sich unbefugt Zugang zu einem Computer oder Informationssystem zu verschaffen. In der Regel geschieht dies durch abgefangene Passwörter oder durch die Nutzung von Insiderinformationen vom Zugangsberechtigten; vgl. *Hecker*, Europäisches Strafrecht, Kap. 11 Rn. 91. Obwohl sich der Begriff des „Hacking-Paragrafen“ im Sprachgebrauch festgesetzt hat, stellen freilich auch viele weitere spezifische Angriffstechniken (z. B. durch Würmer oder Trojaner) einen rechtswidrigen Zugang zu Informationssystemen dar.

[84] Auch der das sog. Hacking betreffende § 202a des deutschen StGB erfüllt die EU-Vorgaben an dieser Stelle trotz einer Gesetzänderung im Jahre 2007 nicht. Dazu sogleich, Kap. 3 § 11 C.

II. Rechtswidriger Systemeingriff

Im Unterschied zum Hacking zielt Art. 4[85] nicht auf die Verletzung der Vertraulichkeit von Informationssystemen oder Computerdaten, sondern verlangt die Kriminalisierung von Schädigungshandlungen gegenüber Informationssystemen. Klassisches Beispiel sind die sog. DoS- (Denial of Service) oder DDoS-Attacken (Distributed Denial of Service) gegenüber einem Server. Dabei wird ein Betriebssystem, ein Internetzugang oder ein anderer Dienst eines Hosts durch eine Vielzahl von Anfragen derartig überlastet, dass er seine eigentliche Funktion nicht mehr auszuführen vermag.[86]

Eine selbstständige Strafbarkeit neben dem „Hacking" wurde deswegen als notwendig erachtet, da ein Eindringen in das betroffene Informationssystem nicht zwingend ist, um dessen Funktionsfähigkeit zu beeinträchtigen oder gar außer Kraft zu setzen. Aus technischer Perspektive muss man sich die Situation dergestalt vorstellen, dass ein massenhafter Aufruf einer Internetseite unternommen wird, der dazu führt, dass reguläre Besucher einer Webseite keinen Zutritt erhalten können. Faktisch wird daher der Zugang lediglich rein „äußerlich" blockiert, sodass ein Eindringen nicht zwingend gegeben ist.

III. Rechtswidriger Eingriff in Daten

Art. 5[87] verlangt die Kriminalisierung des unbefugten Dateneingriffs und unterscheidet sich daher von Art. 4 durch die unterschiedlichen Tatobjekte. Nicht die schwere Behinderung oder Störung eines Informationssystems ist hinreichend, sondern vielmehr wird eine Beeinträchtigung der Computerdaten innerhalb des Informationssystems gefordert. Ob sich der Unterschied zwischen Art. 4 und Art. 5 allerdings in der Praxis auswirkt, darf durchaus bezweifelt werden, da eine schwere Behinderung oder Störung nach Art. 4 oftmals auch

---

[85] Art. 4 der Richtlinie 2013/40/EU: „Die Mitgliedstaaten treffen die erforderlichen Maßnahmen, um sicherzustellen, dass die vorsätzliche und unbefugte schwere Behinderung oder Störung des Betriebs eines Informationssystems durch Eingeben von Computerdaten, durch Übermitteln, Beschädigen, Löschen, Beeinträchtigen, Verändern und Unterdrücken von Computerdaten und durch Unzugänglichmachen von Computerdaten zumindest dann unter Strafe gestellt wird, wenn kein leichter Fall vorliegt."

[86] Für die Rechtslage in Deutschland arbeitet *Valerius*, in: Hilgendorf (Hrsg.), IT-Recht, S. 19 (32 ff.) anhand des „Lufthansa-Falls" (AG Frankfurt a. M. MMR 2005, 863 sowie OLG Frankfurt a. M. MMR 2006, 547, jeweils mit Anmerkungen dazu von *Gercke, M.*) die Strafbarkeit von DDoS-Angriffen als sog. virtuelle Sit-ins umfangreich auf.

[87] Art. 5 der Richtlinie 2013/40/EU: „Die Mitgliedstaaten treffen die erforderlichen Maßnahmen, um sicherzustellen, dass das vorsätzliche und unbefugte Löschen, Beschädigen, Beeinträchtigen, Verändern, Unterdrücken von Computerdaten eines Informationssystems und das Unzugänglichmachen solcher Daten zumindest dann unter Strafe gestellt wird, wenn kein leichter Fall vorliegt."

zumindest eine Unterdrückung oder ein Unzugänglichmachen von Computerdaten innerhalb dieses Informationssystems darstellen wird.[88]

Beispiel: Die DDoS-Attacke auf einen Webserver, bei welcher die auf diesem liegenden Daten nicht mehr zugänglich sind, ist sowohl von Art. 4 als auch von Art. 5 erfasst, da nicht nur eine schwere Beeinträchtigung des Systems, sondern regelmäßig auch eine Unterdrückung der in diesem System gespeicherten Daten gegeben sein dürfte. Ein relevanter Unterschied zwischen den beiden Strafbarkeiten liegt hingegen dann vor, wenn ein System derart angegriffen und gestört wird, dass zwar die Voraussetzungen des Art. 4 erfüllt sind, die gespeicherten Daten jedoch weiterhin erreichbar bleiben.

IV. Rechtswidriges Abfangen von Daten

Die Vorschrift des Art. 6[89] ist gegenüber dem Rahmenbeschluss neu aufgenommen worden und ähnelt Art. 3 der Cybercrime Convention. Anders als Art. 3 der Richtlinie, der es erfordert, den unbefugten Zugang zu Informationssystemen unter Strafe zu stellen, und damit bereits die Integrität des Informationssystems selbst und nicht erst die der Computerdaten schützt, zielt Art. 6 auf den Schutz von Daten während der Übermittlung ab, was hier durch den Begriff des „Abfangens" verdeutlicht wird. Durch Art. 6 der Richtlinie 2013/40/EU wird demnach der Fall angesprochen, dass ein Angreifer weder in ein Computersystem eindringt, noch den Zugriff auf andere Art verhindert, sondern stattdessen lediglich zwischen verschiedenen Computer(systeme)n die übermittelten Daten abfängt. Letztlich handelt es sich somit eher um einen Fall des „Datendiebstahls" als den einer „technischen Computersachbeschädigung".

V. Tatwerkzeuge

Besonders interessant, wenn auch lediglich nüchtern mit „Tatwerkzeuge" betitelt, ist Art. 7 der Richtlinie[90], der abermals Vorgaben der Cybercrime Convention aufgreift und einen weiteren Fall der Vorfeldstrafbarkeit im Computerstraf-

---

[88] Vgl. dazu auch *Sieber*, in: ders./Satzger/von Heintschel-Heinegg (Hrsg.), Europäisches Strafrecht, § 24 Rn. 79.

[89] Art. 6 der Richtlinie 2013/40/EU: „Die Mitgliedstaaten treffen die erforderlichen Maßnahmen, um sicherzustellen, dass das vorsätzliche und unbefugte, mit technischen Hilfsmitteln bewirkte Abfangen nichtöffentlicher Computerdatenübermittlungen an ein Informationssystem, aus einem Informationssystem oder innerhalb eines Informationssystems einschließlich elektromagnetischer Abstrahlungen aus einem Informationssystem, das Träger solcher Computerdaten ist, zumindest dann unter Strafe gestellt wird, wenn kein leichter Fall vorliegt."

[90] Art. 7 der Richtlinie 2013/40/EU: „Die Mitgliedstaaten treffen die erforderlichen Maßnahmen, um sicherzustellen, dass das vorsätzliche und unbefugte Herstellen, Verkaufen, Be-

recht darstellt. Unter Strafe zu stellen ist demnach u. a. die Herstellung von Computerprogrammen, -passwörtern, Zugangscodes und ähnlichen Daten, wenn dies mit der Absicht erfolgt, Straftaten nach den vorgenannten Art. 3–6 zu begehen. Da derartige Verhaltensweisen nach der vorherigen Rechtslage lediglich als Beihilfehandlungen zum Volldelikt[91] strafrechtlich relevant waren, hing eine Strafbarkeit des Verhaltens letztlich vom Erfolgseintritt der Bezugstat ab, was nach den Wertungen des Europarats und des deutschen Strafgesetzgebers der Gefährlichkeit des Verhaltens nicht hinreichend gerecht wurde.[92] Bezüglich dieser Strafbarkeitsbegründung wird auf die folgende intensive Auseinandersetzung mit der Rechtmäßigkeit von Vorfelddelikten aus nationalstaatlicher und unionsrechtlicher Perspektive verwiesen.[93] Positiv wird hingegen regelmäßig aufgenommen, dass die Vorschrift den Mitgliedstaaten die Möglichkeit lässt, flexibel auf die sog. *dual-use*-Problematik zu reagieren.[94]

VI. Anstiftung, Beihilfe und Versuch

Im Rahmen von Art. 8 ist vor allem beachtenswert, dass ausschließlich hinsichtlich Art. 4 und 5 eine Versuchsstrafbarkeit gefordert wird, was zu der paradoxen Situation führt, dass zwar durch Art. 7 das Herstellen, Inverkehrbringen etc. von Tatwerkzeugen zur Begehung von Straftaten i. S. d. Art. 3 und 6 unter Strafe zu stellen sind, der Versuch der entsprechenden Straftaten allerdings nicht. Damit liegt eine Vorbereitungsstrafbarkeit vor, ohne dass das nachgelagerte Versuchsstadium strafbar wäre. Auch für das deutsche Strafrecht wurde diese Konstruktion übernommen. Eine weitere Vertiefung dieser Auffälligkeit kann hier jedoch unterbleiben, da sich Kommentarliteratur und Wissenschaft bereits ausführlich mit dieser Frage auseinandergesetzt haben, seit die internationale Vorgabe in das deutsche Computerstrafrecht umgesetzt worden ist.[95]

---

schaffen zwecks Gebrauchs, Einführen, Verbreiten oder anderweitige Verfügbarmachen folgender Instrumente, das mit der Absicht erfolgt, eine Straftat im Sinne der Artikel 3 bis 6 zu begehen, zumindest dann unter Strafe gestellt wird, wenn kein leichter Fall vorliegt: a) eines Computerprogramms, das in erster Linie dafür ausgelegt oder hergerichtet worden ist, eine Straftat im Sinne der Artikel 3 bis 6 zu begehen; b) eines Computerpassworts, eines Zugangscodes oder ähnlicher Daten, die den Zugang zu einem Informationssystem als Ganzem oder zu einem Teil davon ermöglichen."

[91] Zum Begriff des Volldelikts siehe unten, Kap. 3 § 12 C.

[92] BT-Drs. 16/3656, S. 12.

[93] Siehe unten, Kap. 3 § 12 D. I. 1.

[94] *Sieber*, in: ders./Satzger/von Heintschel-Heinegg (Hrsg.), Europäisches Strafrecht, § 24 Rn. 81.

[95] Siehe u. a. *Borges/Stuckenberg/Wegener*, DuD 2006, 275; *Gröseling/Höfinger*, MMR 2007, 626 (628); *Kargl*, in: NK-StGB Bd. 2, § 202c Rn. 3.

C. Umsetzungsstand in Deutschland

Nachbesserungsbedarf wird für das materielle Strafrecht in Deutschland kaum gesehen. Teilweise wird dies darauf zurückgeführt, dass deutsche Regierungsvertreter und Wissenschaftler bereits von Beginn an bei der Ausarbeitung internationaler Regelungen zur Bekämpfung der Computerkriminalität beteiligt gewesen sind.[96] Diese Regelungen basierten daher entweder in Teilen auf dem deutschen Strafrechtsstandard oder wurden schon frühzeitig national umgesetzt.[97]

Das materielle Computerstrafrecht steht dementsprechend in Deutschland bereits weitestgehend mit der Richtlinie in Einklang. Lediglich in Detailfragen besteht weiterer Harmonisierungsbedarf. Das betrifft etwa den Umstand, dass die deutsche Regelung des Ausspähens von Daten nach § 202a StGB zwar den Anforderungen des rechtswidrigen Zugangs zu Informationssystemen nach Art. 3 der Richtlinie nahezu umfassend gerecht wird, jedoch den tatsächlichen Zugang zu Daten verlangt, was dem beabsichtigten Charakter eines abstrakten Gefährdungsdelikts zuwiderläuft.[98] Weitere Anpassungen sind bei der Bestrafung von qualifizierten Begehungsformen und erschwerenden Umständen notwendig, da die deutschen Höchststrafen in einigen Fällen in Anbetracht der Richtlinien-Vorgaben nicht ausreichen.[99]

Im Falle der sog. *dual-use*-Problematik besteht im deutschen Strafrecht wiederum eigentlich die Notwendigkeit einer Strafbarkeitsbeschränkung, da das deutsche Recht zumindest dem Wortlaut nach strenger ist, als es die EU-Richtlinie vorgibt. Zwar ist es den Mitgliedstaaten grundsätzlich nicht verboten, über die Vorgaben einer EU-Richtlinie hinauszugehen und weitergehende Tatbestände zu schaffen, jedoch bietet die Richtlinie insbesondere beim Einsatz von Schadsoftware sinnvolle Einschränkungsoptionen der Strafbarkeit durch Vorsatzerfordernisse, die das deutsche Strafrecht nicht beinhaltet. Dort wird nämlich von Absicht, mithin dem dolus directus ersten Grads gesprochen, während der § 202c StGB dolus eventualis genügen lässt. Bislang deuten allerdings lediglich Anmerkungen der Bundesregierung[100] und restriktive Auslegungsvorgaben

---

[96] *Sieber*, in: ders./Satzger/von Heintschel-Heinegg (Hrsg.), Europäisches Strafrecht, § 24 Rn. 90.

[97] Als Beispiel dienen die aktuellen internationalen Regelungen zum unbefugten Zugang zu Informationssystemen, die in Deutschland schon 1986 durch das 2. WiKG eingeführt wurden, nachdem die OECD einschlägige Empfehlungen abgegeben hatte; siehe dazu *Sieber*, Informationstechnologie und Strafrechtsreform, S. 31 ff.

[98] *Gröseling/Höfinger*, MMR 2007, 549 (551).

[99] *Sieber*, in: ders./Satzger/von Heintschel-Heinegg (Hrsg.), Europäisches Strafrecht, § 24 Rn. 102.

[100] BT-Drucks. 16/3656, S. 12.

des Bundesverfassungsgerichts auf eine Begrenzung des Tatbestands hin.[101] Sinnvoll wäre es demgemäß, IT-Sicherheitsexperten die Arbeit zu erleichtern, indem bereits im Tatbestand deutlich gemacht wird, dass der Umgang mit *dual-use*-Software nur dann strafbar ist, wenn dabei die Begehung eines eigenen oder fremden Computerdelikts *beabsichtigt* ist.[102]

Beispiel: Der IT-Sicherheitsexperte S schreibt ein Computerprogramm, mit welchem TAN-Kombinationen von Kunden einer großen Bank ausgelesen werden können. Bevor er es letztlich den IT-Abteilungen der Banken für interne Sicherheitssimulationen anzubieten gedenkt, diskutiert er das Softwaredesign mit befreundeten Experten. Ihm ist dabei durchaus bewusst, dass nicht auszuschließen ist, dass jene Experten diese Software auch für illegale Aktivitäten nutzen.

Die derzeitige deutsche Rechtslage klammert diese Fallkonstellation nicht explizit aus dem Anwendungsbereich des § 202c StGB aus, sodass möglicherweise relevante Entwicklungen im Bereich der IT-Sicherheit aus Angst der Programmierer vor Strafbarkeit unterbleiben.

D. Subsumtion unter den netzwerkorientierten Computerkriminalitätsbegriff

Die Richtlinie stellt einen wichtigen Baustein in der Entwicklung der EU im Bereich der Computerkriminalität dar. Die von ihr aufgegriffenen Tatbestände finden sich sämtlich so oder in ähnlicher Form auch in der Cybercrime Convention wieder und die Richtlinie nimmt in Erwägungsgrund 15 nicht nur Bezug auf jene Konvention, sondern stellt sich sogar bewusst in deren Tradition und erklärt deren Ratifizierung durch alle Mitgliedstaaten der EU zum Ziel. Deutlich wird vor allem, dass die digitale europäische Infrastruktur mit flankierenden strafrechtlichen Mitteln abgesichert werden soll.

Über diese allgemein wünschenswerten Aspekte hinaus zielen sämtliche zu harmonisierenden Straftaten der Richtlinie auf digitale Angriffe auf Informationssysteme ab und beziehen sich somit auf eine enge Definition der Computerkriminalität. Dabei nehmen die Delikte nicht nur *alternativ* auf Computer(systeme) als Angriffsmittel oder -objekte Bezug, was die herrschenden Auffassungen genügen lassen,[103] sondern kriminalisieren Handlungen, die eine

---

[101] *Höfinger*, ZUM 2009, 751 (752 f.).

[102] Siehe etwa *Kargl*, in: NK-StGB Bd. 2, § 202c Rn. 7; a. A. wohl *Schumann*, NStZ 2007, 676 (678 f.), der allerdings auch verdeutlicht, dass der Eventualvorsatz nur unter Berücksichtigung des gesetzgeberischen Ziels, der Eindämmung von gefährlichen Verhaltensweisen, sachgerecht ist.

[103] Vgl. oben, Kap. 2 § 4 A.

kumulative Funktion von Computer(systeme)n als Angriffsmittel und -objekte voraussetzen. Sowohl der Netzwerkaspekt dieser Delikte als auch der Schutz klassischer computerspezifischer Rechtsgüter stehen damit im Vordergrund und es besteht durchaus Grund zur Annahme, dass die mit der Richtlinie aufgegriffenen Straftaten keine Rücksicht auf nationale Räume nehmen. Vielmehr ist eher davon auszugehen, dass rein nationale Sachverhalte in Zukunft zufällige Momentaufnahmen sein werden. Insbesondere auch die strafrechtliche Absicherung der europäischen digitalen Infrastruktur gegen digitale Angriffe ist mit guten Gründen dem Kompetenztitel des Art. 83 Abs. 1 UAbs. 2 AEUV zu unterstellen. Die potenziellen Taten bedrohen durch die digitale Vernetzung untereinander nicht mehr ausschließlich einzelne Netzwerke, sondern die gesamte Infrastruktur in der EU und letztlich sogar darüber hinaus. So ist ein Serverausfall bei einem italienischen Telekommunikationsunternehmen nicht nur für jenes, sondern möglicherweise auch für Telekommunikationsinfrastrukturanbieter anderer Mitgliedstaaten von Bedeutung. Vor allem auch der Umstand, dass die digitale Infrastruktur erst die Funktionsfähigkeit vieler kritischer Infrastrukturen[104] sicherstellt, macht sie gewissermaßen selbst zu einer kritischen und damit besonders schutzwürdigen Infrastruktur.[105] Durch die fortschreitende Vernetzung von immer mehr Lebensbereichen haben somit auch lokale Angriffe oftmals EU-weite Auswirkungen, sodass im Rahmen einer typisierenden Betrachtung eindeutig von grenzüberschreitender und besonders schwerer Kriminalität gesprochen werden kann.

Diese vielfach auch als CIA-Delikte[106] klassifizierten Straftaten der Richtlinie sind mithin eindeutig vom hier vertretenen netzwerkspezifischen europäischen Rechtsbegriff der Computerkriminalität des Art. 83 Abs. 1 UAbs. 2 AEUV erfasst.

E. Unterschiede zur Cybercrime Convention

Nicht nur aufgrund des kontinentalen Bezugs zwischen Europäischer Union und Europarat ist dessen Cybercrime Convention an dieser Stelle als Instrument gegen Computerkriminalität aufzunehmen. Insbesondere auch die Tatsache, dass die EU den Einfluss der Vorarbeiten des Europarates auf ihre Politiken zur Bekämpfung von Computerkriminalität ausdrücklich betont, macht einen Über-

[104] Zum Begriff siehe unten, Kap. 4 § 13.

[105] Eine intensive Auseinandersetzung mit dieser Thematik findet sich unten, Kap. 4 § 13 A.

[106] Siehe bereits oben, Kap. 2 § 5 A.

blick[107] und einen Vergleich der jeweiligen Zielrichtungen[108] zwischen der Konvention und der EU-Richtlinie an dieser Stelle lohnenswert. Darüber hinaus wird die Cybercrime Convention zwar aus unterschiedlichen Gründen und von verschiedenen internationalen Akteuren immer wieder kritisiert, stellt jedoch nichtsdestotrotz bislang den umfassendsten und internationalsten Ansatz zur Harmonisierung des Computerstrafrechts dar.

I. Cybercrime Convention im Überblick

Das Instrument mit der größten internationalen Reichweite zur Harmonisierung des formellen und materiellen Computerstrafrechts ist durch den Europarat ausgearbeitet und aktuell von 57 Staaten unterzeichnet und von 53 Staaten ratifiziert worden.[109] Als sog. offenes völkerrechtliches Abkommen können der Konvention nicht nur Mitgliedstaaten des Europarats, sondern auch Drittstaaten beitreten.[110] Obgleich sie vollwertige Mitglieder des Europarates sind, haben Andorra, Griechenland, Irland, Liechtenstein, Monaco und Schweden die Cybercrime Convention nach ihrer Unterzeichnung bislang nicht umgesetzt. Russland und San Marino gehören darüber hinaus nicht einmal zur Gruppe der Unterzeichnerstaaten.

Der Europarat gibt unter Berufung auf interne Quellen an, dass die tatsächliche Wirkung der Cybercrime Convention weit über die Unterzeichnerstaaten hinausreicht, da sich die computerstrafrechtliche Gesetzgebung weltweit in mehr als 100 Staaten direkt oder indirekt an der Konvention orientiert.[111] Auch wenn eine Überprüfung dieser Angaben nicht ohne Weiteres möglich ist, kann davon ausgegangen werden, dass viele Staaten bei der Implementierung computerstrafrechtlicher Normen auf die Inhalte der Cybercrime Convention zurückgreifen.[112]

1. Aufbau der Konvention

Im ersten Abschnitt des zweiten Kapitels benennt die Konvention Delikte, die gegen oder durch Computernetzwerke verübt werden. Genannt sind einerseits

---

[107] Siehe sogleich unten, Kap. 3 § 11 E. I.

[108] Siehe unten, Kap. 3 § 11 E. II.

[109] Stand: März 2017.

[110] Die Nicht-Mitglieder Australien, die Dominikanische Republik, Japan, Mauretanien, Panama und die Vereinigten Staaten von Amerika haben die Konvention bereits ratifiziert, während Kanada und Südafrika bislang lediglich unterzeichnet haben.

[111] Contribution of the Secretary General of the Council of Europe to the 12th United Nations Congress, ID SG/Inf(2010)4, 2010, S. 18.

[112] *Gercke, M.*, Computer Law Review International 2011, 142 (143) auch m. w. N. zu einzelnen Staaten (Argentinien, Botswana, Ägypten, Nigeria, Pakistan und die Philippinen).

der rechtswidrige Zugang zu Computersystemen (Art. 2), das rechtswidrige Abfangen übertragener Computerdaten (Art. 3), Eingriffe in Daten (Art. 4), Eingriffe in Computersysteme (Art. 5) und der Missbrauch von Vorrichtungen (Art. 6) als solche Straftaten, die gegen die Vertraulichkeit, Unversehrtheit und Verfügbarkeit von Daten und Systemen begangen werden und bei denen Computersysteme das Angriffsobjekt darstellen.[113] Andererseits werden Straftaten identifiziert, bei denen Computernetzwerke als Tatwerkzeug eingesetzt werden. Dazu zählen neben der computerbezogenen Fälschung (Art. 7) und dem computerbezogenen Betrug (Art. 8) auch inhaltsbezogene Delikte, wie Straftaten mit Bezug zu Kinderpornografie (Art. 9).[114] Lediglich in einem Zusatzprotokoll[115] sind darüber hinaus Vorgaben festgehalten, um rassistische und fremdenfeindliche Taten in Computersystemen unter Strafe zu stellen, da ein Konsens auf diesem Gebiet nicht zwischen allen Unterzeichnerstaaten hergestellt werden konnte. Der materielle Teil des Übereinkommens schließt mit Straftaten im Zusammenhang mit Verletzungen des Urheberrechts und verwandter Schutzrechte (Art. 10).

Im zweiten Abschnitt des zweiten Kapitels wird auch eine verfahrensrechtliche Harmonisierung der Rechtsordnungen in den jeweiligen Unterzeichnerstaaten angestrebt. In den Art. 16 und Art. 17 wird die beschleunigte Sicherung von Computer- bzw. Verkehrsdaten behandelt, während sich Art. 18 der Anordnung der Herausgabe von Kundendaten und Art. 19 den Vorgaben zur Durchsuchung und Beschlagnahme von Computerdaten widmen. Art. 20 und Art. 21 schließlich sehen eine Pflicht zur Echtzeiterhebung von Verkehrs- bzw. Inhaltsdaten vor. Art. 15 setzt bezüglich der aufgezählten Maßnahmen Bedingungen und Garantien, die die Vertragsparteien an die Beachtung der Menschenrechte und der Grundfreiheiten nach der EMRK erinnern und stellt somit hinsichtlich der Grundsätze der Verhältnismäßigkeit und der gerichtlichen Verfahrenskontrolle Mindeststandards dar. Vor allem aufgrund fehlender spezifischer Eingriffsschranken für die Strafverfolgungsbehörden unter Berücksichtigung von Datenschutzgesichtspunkten[116] sowie Beschuldigtenrechten[117] ist dieser Abschnitt des Übereinkommens nicht unumstritten geblieben.

---

[113] *Hilgendorf/Valerius*, Computer- und Internetstrafrecht, § 1 Rn. 122.

[114] Zu den unterschiedlichen Zielen von Cybercrime Convention (ETS Nr. 185) und EU-Richtlinien sowie den damit verbundenen Definitionsabweichungen bzgl. des Computerkriminalitätsbegriffs siehe Kap. 3 § 11 E. II.

[115] Zusatzprotokoll zur Kriminalisierung von Handlungen rassistischer und fremdenfeindlicher Art begangen durch Computersysteme v. 28.1.2003 (ETS Nr. 189).

[116] Siehe *Breyer*, DuD 2001, 592 (595 ff.)

[117] *Valerius*, K&R 2004, 513 (517 f.).

Den dritten maßgeblichen Teil des Übereinkommens stellt schließlich der erste Abschnitt des dritten Kapitels dar. Dieser widmet sich der internationalen Zusammenarbeit in den Bereichen Auslieferung und Rechtshilfe. Insbesondere ist hier die allgemeine Handlungsanweisung des Art. 23 zu nennen, die eine Zusammenarbeit „in größtmöglichem Umfang" einfordert, die in den Art. 24 ff. inhaltlich konkretisiert wird.

2. *Umsetzungsstand und aktueller Diskurs*

Der unmittelbare Anpassungsbedarf des deutschen Strafrechts im Hinblick auf die Vorgaben der Cybercrime Convention stellte sich in seinen Ausmaßen zwar als einigermaßen gering dar,[118] ist in der Intensität, vor allem wegen der noch zu behandelnden Vorverlagerung von Strafbarkeiten,[119] allerdings vielfach kritisiert worden.

Ob es die Cybercrime Convention allerdings tatsächlich vermag, in den kommenden Jahren einen massiven Anstieg an Ratifikationen zu verzeichnen, um dadurch tatsächlich ein globales Instrument zur Harmonisierung des Computerstrafrechts zu werden, darf durchaus bezweifelt werden. Die Mitglieder der Konvention sind größtenteils der sog. entwickelten Welt zuzurechnen. Insbesondere einflussreiche Entwicklungs- und Schwellenländer fehlen bislang in der Liste der Unterzeichnerstaaten. Brasilien,[120] Russland (obwohl es Mitglied des Europarats ist!) und China etwa haben bereits deutlich gemacht, dass von ihnen eine Unterzeichnung der Konvention auch in Zukunft nicht zu erwarten ist. Bei Russland ist die Ablehnung darauf zurückzuführen, dass durch den transnationalen Datenzugriff nach Art. 32 der Konvention die Souveränitätsrechte der Unterzeichnerstaaten beeinträchtigt werden.[121] China lehnt eine Unterzeichnung vor allem wegen fehlender Konformität mit dem nationalen Strafrecht und aufgrund der Tatsache ab, dass es bei der Erarbeitung der Konvention nicht konsultiert worden ist.[122] Damit unterfällt der Internetverkehr von mehr als 50 Prozent der weltweiten Nutzer nicht der Cybercrime Convention.[123] Dieser Befund ist insbesondere deswegen bemerkenswert und hinsichtlich der globalen Wirkung der Cybercrime Convention problematisch, weil neben dem Bevölke-

---

[118] *Hilgendorf/Valerius*, Computer- und Internetstrafrecht, § 1 Rn. 126.

[119] Siehe im Detail dazu unten, Kap. 3 § 12.

[120] Brasiliens Vorbehalte beziehen sich u. a. auf sie Kriminalisierung von Urherrechtsverstößen; siehe *Harley*, Columbia Science and Technology Law Review, XI, 2013; abrufbar unter: http://www.stlr.org/2010/03/a-global-convention-on-cybercrime/ (Stand: 07.08.2017).

[121] Computer Crime Research Center, 'Putin defies convention on cybercrime'; abrufbar unter: http://www.crime-research.org/news/28.03.2008/3277 (Stand: 07.08.2017).

[122] Siehe dazu im Einzelnen *Chang*, Cybercrime, S. 125.

[123] *Broadhurst/Chang*, in: Liu/Hebenston/Jou (Hrsg.), Criminology, S. 58.

rungswachstum in den oben genannten Ländern auch vor allem deren digitale Präsenz mit großer Geschwindigkeit voranschreitet.

Die Gründe, die hinter der Entscheidung eines Staats gegen Harmonisierungsanstrengungen stehen, sind vielschichtig.[124] Sie reichen von verfassungsrechtlichen Bedenken über föderal-rechtliche Probleme bis hin zu religiös-rechtlichen Unvereinbarkeiten (Sharia) von internationalem Computerstrafrecht mit nationalstaatlichen Regelungen.[125] Aktuelle Entwicklungen sprechen also durchaus dafür, dass die Zahl der Unterzeichnerstaaten in naher Zukunft keinen großen Sprung machen wird und insbesondere die Teilnahme von wichtigen Entwicklungs- und Schwellenländern auf längere Sicht unwahrscheinlich ist.

II. Vergleich: „core cybercrime approach“ vs. „comprehensive approach“

Im Gegensatz zum Ansatz der Cybercrime Convention, alle mit der Computernutzung in Zusammenhang stehenden Deliktsbereiche in einem möglichst global gültigem Instrument zu erfassen (sog. *comprehensive approach*) geht die Richtlinie 2013/40/EU einen etwas anderen Weg. Zwar basieren ihre computerstrafrechtlichen Vorgaben an die Mitgliedstaaten, teilweise wortgleich, auf der Cybercrime Convention, allerdings bildet die Richtlinie nur einen Teil der nach der Konvention anzugleichenden Delikte ab. Lediglich der Kernbereich des Computerstrafrechts, namentlich die sog. CIA-Delikte, wird erfasst.

Im Rahmen von internationalen Anstrengungen zur Harmonisierung des Computerstrafrechts wurde in der Vergangenheit regelmäßig nach einem *comprehensive approach* verlangt,[126] also nach einem völkerrechtlichen Abkommen oder einem *model law*, das sämtliche denkbare Bereiche der Computerkriminalität regelt. Dass dabei oftmals die weiteste Begriffsbestimmung („Jede Straftat, die unter Verwendung eines oder gegen ein computerbasiertes Endgerät gerichtet ist.“) im Hinblick auf die Computerkriminalität Anwendung findet, ist in diesem Zusammenhang auch weit weniger problematisch als im Rahmen der EU-rechtlichen Harmonisierung. Die Bindungswirkung völkerrechtlicher Abkommen und *model laws* ist schließlich nicht mit derjenigen von Richtlinien nach Art. 83 Abs. 1 UAbs. 2 AEUV vergleichbar.

Harmonisierungsansätze mit einem Fokus auf einzelne Aspekte der Computerkriminalität hätten allerdings auch im völkerrechtlichen und *soft-law*-

---

[124] Auch *Seger*, in Manacorda (Hrsg.), Cibercriminality, S. 167 (174 f.) führt unterschiedliche Erklärungsansätze für die stockende globale Ausbreitung der Cybercrime Convention an.

[125] *Sieber u. a.*, Comprehensive Study on Cybercrime, 2013, S. 58 m. w. N.

[126] Etwa *Gercke, M.*, Understanding Cybercrime Studie, 2012, S. 3; aber auch die Cybercrime Convention verfolgte dieses Ziel; vgl. die Aussage des Generalsekretärs des Europarates beim 12. Strafrechtskongress der Vereinten Nationen, ID SG/Inf(2010)4, 2010, Nr. 47.

Bereich gewisse Vorteile. Sie böten auch solchen Staaten die Möglichkeit, die internationale Rechtsangleichung voranzutreiben, denen ein umfassender Ansatz verfassungsrechtliche Probleme bereitet. Insbesondere der Umstand, dass die meisten nationalen (verfassungs-)rechtlichen Konflikte und Harmonisierungshindernisse im Bereich der Computerkriminalität i. w. S (v. a. bei den inhaltsbezogenen und gegen das Urheberrecht gerichteten Delikten) auftreten, spricht auch im Bereich völkerrechtlicher Abkommen und bei Bemühungen um internationale *model laws* zur Computerkriminalität zunächst für eine Konzentration auf den Bereich der Computerkriminalität i. e. S.[127]

Das formelle und materielle Strafrecht stellt sowohl mit seinen Präventiv- als auch mit seinen Repressivfunktionen einen wichtigen Baustein in der (über-) staatlichen Sicherheitsarchitektur dar. In einem transnationalen Kriminalitätsbereich wie dem der Computerkriminalität ist – wie bereits ausgeführt[128] – die bestmögliche Einsatzfähigkeit und Schlagkräftigkeit des materiellen Strafrechts durchaus von einer weitgehenden internationalen Harmonisierung abhängig. Informationssysteme sind in einer globalisierten und zunehmend vernetzten Welt besonders verletzliche Angriffspunkte. Ihre ständige Funktionsfähigkeit ist allerdings auch teilweise konstituierend für einen Staat und eine sichere Gesellschaft. Daher ist der Ansatz der EU, zunächst diesen Kernbereich der Computerkriminalität zu harmonisieren, zu unterstützen. Zwar ist eine weltweite Einigung auf computerstrafrechtliche Grundsätze nach einem weiten Verständnis durchaus wünschenswert, jedoch sind zum jetzigen Zeitpunkt Maßnahmen angezeigt, die den Kernbereich der Computerkriminalität international angleichen, um den bekannten Problemen und Hindernissen (*safe havens*, *dual criminality* etc.) zumindest hier zu begegnen.

Eine Vereinbarung mit dem EU-Kompetenzrecht ist selbstverständlich keine Voraussetzung für die Rechtmäßigkeit eines völkerrechtlichen Abkommens. Nach der hier vertretenen Auffassung wäre eine solche Vereinbarkeit darüber hinaus aber auch nicht gegeben, da die Cybercrime Convention nicht mit einer engen, netzwerkspezifischen und auf den Schutz computerspezifischer Rechtsgüter konzentrierten Definition der Computerkriminalität arbeitet, sondern stattdessen auf eine umfassende Angleichung des formellen und materiellen Strafrechts bei Delikten mit Bezug zu Computern abzielt.

---

[127] Weiterführend zur Thematik siehe *Haase*, in: IEEE Xplore Digital Library (ICACC 2015), S. 1 ff.

[128] Vgl. oben, Kap. 2 § 7 A.

§ 12 Vorfeldstrafbarkeiten im Computerstrafrecht

Trotz der kompetenzrechtlichen Zustimmung zur Richtlinie hinsichtlich des Begriffs der Computerkriminalität bietet der Inhalt derselben mit der weitreichenden Einführung einer Vorbereitungsstrafbarkeit ein strafrechtsdogmatisches Problem. Die Frage der Rechtmäßigkeit einer Kriminalisierung von Vorbereitungshandlungen stellt sich selbstverständlich nicht ausschließlich im Rahmen des Computerstrafrechts. Die Anforderungen der Cybercrime Convention und durch ihre noch stärkere Bindungswirkung umso mehr diejenigen der Richtlinie 2013/40/EU bieten allerdings Gelegenheit, sich kritisch mit diesem Phänomen auseinanderzusetzen.

Im Folgenden wird erstens in der gebotenen Kürze das Konstrukt der Vorbereitungsstrafbarkeit aus allgemeiner Perspektive dargestellt, dogmatisch eingeordnet und bezüglich seiner Verfassungsmäßigkeit untersucht.[129] Zweitens werden die gewonnenen Erkenntnisse im Anschluss auf das Computerstrafrecht übertragen und die entsprechende Kritik aufgegriffen[130] und drittens folgt eine eigene Stellungnahme zur Verfassungsmäßigkeit der Vorfeldkriminalisierung im Computerstrafrecht verbunden mit einer Rechtmäßigkeitsüberprüfung der Richtlinie 2013/40/EU.[131]

A. Vorbereitungshandlungen im Strafnormgefüge

Strafrecht dient dem Rechtsgüterschutz.[132] Dieser vielzitierte Grundsatz[133] ist jedem Rechtswissenschaftler hinreichend bekannt. Was aber folgt aus dieser Feststellung? Sie bedeutet, dass gesellschaftlich unerwünschtes Verhalten ausschließlich dann mit Strafe zu bedrohen ist, wenn das Verhalten strafrechtlich anerkannte Rechtsgüter schädigt bzw. (konkret oder abstrakt) gefährdet.[134] Entsprechend diesem Grundsatz werden im deutschen Strafrecht Schädigungsde-

---

[129] Kap. 3 § 12 A.

[130] Kap. 3. § 12 B.

[131] Kap. 3. § 12 C und D.

[132] Auch wenn die ganz h. M. das heute so sieht, sei darauf hingewiesen, dass durchaus namhafte Stimmen diesem Prinzip widersprechen und etwa den Normgeltungsschutz als Legitimationsbasis des modernen Strafrechts bezeichnen; siehe etwa *Jakobs*, Rechtsgüterschutz, S. 19 ff.

[133] Siehe dazu u. a. BVerfGE 39, 1 (46); 45, 187 (253); *Hefendehl*, ZIS 2012, 506 (507); *Heinrich*, Strafrecht AT, Rn. 3; *Kaufmann*, Aufgabe des Strafrechts, S. 5; *Roxin*, Strafrecht AT Bd. 1, § 2 Rn. 1; differenzierend *Kindhäuser*, in: Lüderssen u. a. (Hrsg.), Modernes Strafrecht, S. 29 ff., der noch weiter zwischen Rechtsgütern und Strafrechtsgütern differenziert und nur letztere zum Schutzkreis des Strafrechts zählt.

[134] In anderen Fällen verweist der Gesetzgeber auf zivilrechtliche Ansprüche.

likte und Gefährdungsdelikte unterschieden. Während erstere lediglich die Schädigung eines Rechtsguts strafrechtlich erfassen, ordnen letztere ein zunächst unschädliches Verhalten als so gefährlich ein, dass bereits die konkrete oder sogar nur die abstrakte Gefährdung eines Rechtsguts zur Strafbarkeitsbegründung ausreichen.[135]

Zusätzlich zu den Stadien Vollendung und Beendigung ist bei sämtlichen Verbrechen und in den angeordneten Fällen auch bei Vergehen bereits der Versuch einer Straftat mit Strafe bedroht. Nach der herrschenden und seit einer Gesetzesänderung 1975 allgemein anerkannten gemischt subjektiv-objektiven Versuchstheorie sind bei einem Versuchsdelikt sowohl die rechtsfeindliche Gesinnung des Täters als auch die nach außen gerichtete Manifestation dieser Gesinnung erforderlich.[136] Danach sind subjektiv ein *Tatentschluss* und objektiv ein *unmittelbares Ansetzen* des Täters zur Tatbestandsverwirklichung notwendig.

Diesem Versuchsstadium vorgelagert gibt es noch ganz zu Beginn einer (potenziellen) Deliktsbegehung den sog. inneren Tatentschluss des Täters. Dieser ist immer straflos, da eine Gesinnungsstrafbarkeit dem deutschen Strafrecht fremd ist und somit jeweils eine Manifestation des inneren Entschlusses gegeben sein muss.[137]

Vorliegend besonders interessant ist schließlich das Deliktsstadium der sog. Vorbereitungshandlungen, das zwischen innerem Entschluss und strafrechtlich oftmals relevantem Versuch angesiedelt und grundsätzlich straflos ist.[138] Dabei handelt es sich regelmäßig um strafrechtlich neutrale Handlungen, bei denen eine unmittelbare Rechtsgutsgefährdung noch nicht gegeben ist.[139] Der Gesetzgeber hat von diesem Grundsatz allerdings Ausnahmen geschaffen. Erstens gibt es bestimmte Tatbestände, die Vorbereitungshandlungen strafrechtlich als Vorfeldtatbestände ausdrücklich erfassen und damit rechtlich zunächst neutrale Handlungen durch eine tatsächliche wie normative Verknüpfung zu einem Teil des späteren Volldelikts machen. Zweitens gibt es den Bereich der sog. Mitgliedschafts- oder Organisationsdelikte, wie etwa die Verbrechensverabredung nach § 30 Abs. 2 StGB oder die Bildung krimineller bzw. terroristischer Vereinigungen nach den §§ 129, 129a StGB. Diese stehen gewissermaßen zwischen

---

[135] Zur grundsätzlichen Legitimation abstrakter Gefährdungsdelikte siehe *Graul*, Gefährdungsdelikte, S. 140 ff.; *Kindhäuser*, Gefährdung als Straftat, S. 225 ff.

[136] BGHSt 26, 201 (202); siehe auch *Heinrich*, Strafrecht AT, Rn. 636 m. w. N.

[137] Vgl. *Heinrich*, Strafrecht AT, Rn. 702; *Krey/Esser*, Strafrecht AT, Rn. 1193; *Rath*, JuS 1998, 1006 (1007).

[138] *Eser/Bosch*, in: Schönke/Schröder (Hrsg.), Vor § 22 StGB Rn. 13; *Hillenkamp*, in: LK-StGB, Vor § 22 Rn. 5; *Lackner/Kühl*, StGB, Vor § 22 Rn. 3; *Wessels/Beulke/Satzger*, Strafrecht AT, § 17 Rn. 839.

[139] Statt vieler: *Heinrich*, Strafrecht AT, Rn. 704.

den „reinen“ abstrakten Gefährdungsdelikten und den klassischen Vorbereitungsstraftaten.[140] Sie pönalisieren nämlich einerseits keine unmittelbar auf ein späteres bestimmtes Volldelikt gerichtete Handlung, wie die klassischen Vorbereitungsdelikte, andererseits aber auch nicht lediglich Handlungen, die zur Unbeherrschbarkeit des weiteren Geschehens führen, wie beispielsweise die Trunkenheit im Verkehr. Diese Kategorie der „hybriden“ abstrakten Gefährdungsdelikte kann an dieser Stelle allerdings außen vor bleiben, da man es im Computerstrafrecht ausschließlich mit klassischen Vorbereitungsdelikten zu tun hat, die jedoch wiederum in zwei Untergruppen aufzuteilen sind.[141] Besonders plastisch wird der Vorbereitungscharakter eines Delikts, wenn dieser im Wortlaut der Strafnorm explizit ausgedrückt wird:

Beispiele für klassische Vorbereitungsstrafbarkeiten sind erstens etwa § 80 StGB (Vorbereitung eines Angriffskrieges);[142] *§ 83 StGB (Vorbereitung eines hochverräterischen Unternehmens); §§ 89–89b StGB (Vorbereitung einer schweren staatsgefährdenden Gewalttat und Aufnahme von Beziehungen zur Begehung einer schweren staatsgefährdenden Gewalttat); § 149 StGB (Vorbereitung der Fälschung von Geld oder Wertpapieren); § 234a Abs. 3 StGB (Vorbereitung einer Verschleppung) und § 310 StGB (Vorbereitung eines Explosions- oder Strahlungsverbrechens) sowie aus dem Nebenstrafrecht § 369 I Nr. 3 2. Alt. AO (Vorbereitung der Wertzeichenfälschung) und § 22b I Nr. 3 StVG (Vorbereitung des Missbrauchs von Wegstreckenzählern und Geschwindigkeitsbegrenzern).*

Neben diesen „benannten“ Fällen finde sich im StGB und im Nebenstrafrecht eine Reihe von Vorbereitungsstrafbarkeiten, welche den Begriff der Vorbereitung selbst nicht im Tatbestand führen. Typischerweise beschreiben sie stattdessen Handlungen, die einer Rechtsgutsverletzung vorgelagert sind und daher hier als „unbenannte“ Vorbereitungsdelikte bezeichnet werden sollen.

Beispiele dafür sind etwa § 176 Abs. 4 Nr. 3 StGB (Einwirken auf ein Kind mittels Schriften als Vorbereitung eines sexuellen Missbrauchs nach Abs. 1); § 180 Abs. 1 StGB (Vorschubleisten sexueller Handlungen einer Person unter sech-

[140] So auch *Puschke*, in Hefendehl (Hrsg.), Grenzenlose Vorverlagerung, S. 9 (13).

[141] In seinem Diskussionsbeitrag geht auch *Schroeder*, in: Hefendehl (Hrsg.), Grenzenlose Vorverlagerung, S. 63 (66), auf die Unterscheidung zwischen „ ausdrücklichen Vorbereitungsdelikten“ und solchen Delikten, die erst „infolge wissenschaftlicher Erörterung“ ihren wahren Charakter offenbaren, ein. Für letztere fordert er deshalb eine verfassungsrechtliche Überprüfung anhand einschränkender Kriterien.

[142] Dieser Tatbestand stellt eine Besonderheit dar, da er die Vorbereitung einer Handlung beschreibt, die ihrerseits nicht mit Strafe bedroht ist; siehe dazu *Mitsch*, Straflose Provokation, S. 203.

zehn Jahren); § 219a StGB (Werbung für den Abbruch einer Schwangerschaft als Vorbereitungshandlung für den strafbaren Schwangerschaftsabbruch nach § 218 StGB); § 265 StGB (Versicherungsmissbrauch als Vorbereitung zur späteren Vermögensschädigung zulasten der Versicherung). Auch im Nebenstrafrecht finden sich unbenannte Vorbereitungsdelikte wie etwa § 108b UrhG i. V. m. § 95a UrhG (Unerlaubte Eingriffe in technische Schutzmaßnahmen und zur Rechtewahrnehmung erforderliche Informationen).[143]

Die computerstrafrechtlichen Delikte mit Vorbereitungscharakter fallen dabei in die Kategorie der „benannten" Vorbereitungsstraftaten.[144] § 202c StGB kriminalisiert das Vorbereiten des Ausspähens (§ 202a StGB) und Abfangens (§ 202b StGB) von Daten, die §§ 303a (Datenveränderung) und 303b StGB (Datenveränderung) verweisen jeweils in Abs. 3 hinsichtlich der Strafbarkeit von Vorbereitungshandlungen auf § 202c StGB und auch § 263a Abs. 3 StGB spricht ausdrücklich von der Vorbereitung eines Computerbetrugs.

Es zeigt sich also, dass an einer Vielzahl von Stellen im deutschen Strafrecht Tatbestände aufzufinden sind, die eine Strafbarkeit nicht erst ab dem Erreichen des Versuchsstadiums begründen, sondern bereits vorher ansetzen und die Vorbereitung zu einer Straftat kriminalisieren. Üblicherweise wird angenommen, dass eine solche Instrumentalisierung des Strafrechts zulässig ist, wenn die Hochwertigkeit des betroffenen Rechtsguts und die hohe Gefährlichkeit eines Verhaltens für dieses Rechtsgut festzustellen ist.[145] *Hassemer* etwa ist der Auffassung, „dass die Erweiterung des Rechtsgutschutzes durch Verhaltensdiskriminierung im Vorfeld der Rechtsgutsverletzung sich am Wert des zu schützenden Rechtsguts und/oder an der Intensität seiner Bedrohung legitimieren muss. Eine solche Erweiterung ist nur dann erlaubt, wenn Wert und/oder Bedrohungsintensität hoch sind".[146] Zwar ist diese Ansicht bei Weitem nicht die restriktivste,[147] jedoch ist, wie zu zeigen sein wird,[148] bei der computerstrafrechtlichen Vorfeldkriminalisierung nicht einmal die Einhaltung dieses Grundkonsenses

---

[143] Vgl. zu den verschiedenen Beispielen *Hillenkamp*, in: LK-StGB, Vor § 22 Rn. 8 und *Mitsch*, JURA 2013, 696 (699 f.).

[144] Dies ist zumindest nach der hier vertretenen Definition der Fall. Bei Anlegung eines weiten Begriffsmaßstabs wären u. U. auch unerlaubte Eingriffe in technische Schutzmaßnahmen und zur Rechtewahrnehmung erforderliche Informationen gem. § 108b UrhG i. V. m. § 95a UrhG als Computerdelikte einzuordnen.

[145] Statt vieler: *Hörnle*, GA 2006, 80 (94); *Koriath*, GA 2001, 51 (68); *Schünemann*, in: GS Meurer (2002), S. 37 (59).

[146] *Hassemer*, Soziologie des Verbrechens, S. 220; *Lagodny*, Schranken der Grundrechte, S. 519.

[147] In einem noch erheblich weitergehenden Umfang der Vorbereitungsstrafbarkeit ablehnend gegenüberstehend *Chou*, Vorbereitungsdelikte, insb. S. 145 f.

[148] Siehe unten, Kap. 3 § 12 C.

sichergestellt. Obwohl nach klassischem Verständnis strafrechtliche Mechanismen erst dann greifen, wenn Rechtsgüter bereits geschädigt worden sind,[149] geht die mittlerweile gefestigte verfassungsgerichtliche Rechtsprechung davon aus, dass auch präventive Zielbestimmungen des Strafrechts, und damit auch Vorfeldtatbestände, dem Grundgesetz nicht entgegenstehen.[150] Stattdessen seien auch Strafnormen ausschließlich am verfassungsrechtlichen Verhältnismäßigkeitsprinzip zu messen.[151] Strafrechtsspezifische Prinzipien, wie der Schuld- sowie der tatbestandsbezogene Bestimmtheitsgrundsatz gehen freilich über die allgemeine grundgesetzliche Pflicht zur Verhältnismäßigkeit jeder staatlichen Maßnahme hinaus.[152]

Für die grundsätzliche verfassungsrechtliche Legitimität der Strafbarkeit von Vorbereitungshandlungen führt das Bundesverfassungsgericht zudem Art. 26 Abs. 1 S. 1 und 2 GG ins Feld, der Basis des § 80 StGB (Vorbereitung eines Angriffskrieges) ist und normiert, dass „Handlungen, die geeignet sind und in der Absicht vorgenommen werden, das friedliche Zusammenleben der Völker zu stören, insbesondere die Führung eines Angriffskrieges vorzubereiten, verfassungswidrig [… und] unter Strafe zu stellen [sind]".[153]

Der Auffassung des Bundesverfassungsgerichts, dass damit eine generelle verfassungsrechtliche Offenheit gegenüber strafrechtlichen Vorbereitungsdelikten verbunden sei,[154] kann hier nicht gefolgt werden. Vielmehr könnte man i. S. e. *argumentum e contrario* sogar annehmen, dass Art. 26 Abs. 1 GG lediglich in diesem speziell benannten Fall eine Vorbereitungsstrafbarkeit vorsieht und in allen anderen Fällen deren Verfassungsmäßigkeit mithin zu verneinen wäre. Zwar ist diesem Argument letztlich wiederum entgegenzusetzen, dass Art. 26 GG verfassungsrechtlicher Ausdruck des Friedensgebots ist,[155] und nicht der strafrechtlichen Zielbestimmung des Grundgesetzes dient. Jedoch folgt aus der verfassungsrechtlichen Absicherung des Friedensgebots durch einen Normbefehl zur Kriminalisierung von Vorbereitungshandlungen in Bezug auf einen Angriffskrieg durchaus, dass derartig freiheitssensiblen Maßnahmen

---

[149] U. a. *Heger*, in: Giegerich (Hrsg.), Herausforderungen und Perspektiven der EU, S. 157 und *Sieber*, ZStW 119 (2007), 1 (34), weisen auf diesen klassischen Ansatz kontinentaleuropäisch geprägter Rechtssysteme hin.

[150] Siehe etwa bereits BVerfGE 28, 175 (186 ff.); BVerfG NJW 1993, 1911; BVerfG NVwZ 2006, 583 (584).

[151] BVerfGE 120, 224 (241); das BVerfG weist in seiner Entscheidung explizit darauf hin, dass insbesondere die strafrechtliche Konstruktion des Rechtsgüterschutzes keine zusätzlichen Hürden bei der Beurteilung der Verfassungsmäßigkeit aufzustellen vermag.

[152] Vgl. *Hassemer*, StV 2006, 322, (329 ff.); *Sieber*, ZStW 119 (2007), 1 (36).

[153] BGH NJW 2014, 3459 (3463).

[154] BGH NJW 2014, 3459 (3463).

[155] *Herdegen*, in: Maunz/Dürig (Hrsg.), GG, 76. EL Dez. 2015, Art. 26 Rn. 2.

zumindest besonders hochwertige Schutzgüter gegenüberzustehen haben. Auch das Bundesverfassungsgericht scheint diese Ansicht grundsätzlich zu teilen, da explizit der „Schutz der hochrangigen Individual- und Allgemeinrechtsgüter“[156] als Grundbedingung der Vorfeldkriminalisierung angeführt wird.

Unabhängig von weiteren Voraussetzungen verfassungsgemäßer Vorbereitungsdelikte, wie der objektiven Manifestation des subjektiv Gewollten und der Sicherstellung eines gewissen Zurechnungszusammenhangs zwischen Vorbereitungshandlung und Bezugstat,[157] ist mithin insbesondere die Hochrangigkeit der Schutzgüter als Legitimationskriterium heranzuziehen. Dies folgt zudem nicht lediglich aus mittelbar auf Verfassungsgrundsätze zurückzuführenden strafrechtsspezifischen Prinzipien, sondern entspringt unmittelbar dem Verhältnismäßigkeitsgrundsatz. Während also Vorbereitungsstrafbarkeiten zum Schutz hochrangiger Rechtsgüter grundsätzlich verfassungskonform sein können, ist hingegen der Schutz mittel- oder niedrigrangiger Rechtsgüter durch Vorfeldstrafbarkeiten unverhältnismäßig und daher nicht mit dem Grundgesetz vereinbar.

B. Systematische Kritik an der computerstrafrechtlichen Vorfeldstrafbarkeit

Im Bereich der Kriminalisierung von Vorbereitungshandlungen bieten weder der Rahmenbeschluss noch die aktualisierte Richtlinie relevante Neuerungen zu den Vorgaben der Cybercrime Convention. Da Deutschland die Konvention bereits durch das 41. StrÄndG umgesetzt und anschließend ratifiziert hatte, stellte sich, wie gezeigt, auch der weitere Harmonisierungsbedarf als gering dar. Nichtsdestotrotz wurde und wird insbesondere an der Ausweitung der Strafbarkeit auf Vorbereitungshandlungen bei den computerstrafrechtlichen Delikten massiv Kritik geübt. Diese bezieht sich dabei maßgeblich auf drei Aspekte.

Erstens wird in der Literatur die bereits oben angedeutete Paradoxie aufgezeigt, dass es sich bei den §§ 202a StGB (Ausspähen von Daten) und 202b StGB (Abfangen von Daten) um Vergehen handele, deren Versuchsstrafbarkeit nicht gesetzlich angeordnet ist, gleichzeitig aber durch § 202c StGB Vorbereitungshandlungen zu jenen Straftaten kriminalisiert werden.[158]

---

[156] BGH NJW 2014, 3459 (3463).

[157] Sie insoweit insb. die umfassenden Ausführungen bei *Sieber*, NStZ 2009, 353 (359 ff.).

[158] Vgl. bspw. *Borges/Stuckenberg/Wegener*, DuD 2007, 275; *Ernst*, NJW 2007, 2661 (2662); *Gröseling/Höfinger*, MMR 2007, 626 (628); *Hilgendorf/Valerius*, Computer- und Internetstrafrecht, § 3 Rn. 573; *Kargl*, in: NK-StGB Bd. 2, § 202c Rn. 3; *Schumann*, NStZ 2007, 675 (679).

Beispiel: Hacker H schreibt ein Computerprogramm, das dafür konzipiert und geeignet ist, durch die Überwindung von Zugangsschranken in Computersysteme einzudringen, um darin gesicherte Daten zu erlangen und macht sich dadurch nach §§ 202a, 202c StGB strafbar. Setzt derselbe Hacker dieses Computerprogramm nun aber tatsächlich ein, scheitert er dann jedoch an der Verschlüsselung des „angegriffenen" Computersystems, befindet er sich mangels Erfolgseintritts im straflosen (Versuchs-)Bereich.

Lediglich in Fällen, in denen der Vorfeldtäter ein Programm nicht zur eigenen Verwendung schreibt, sondern um es an einen Dritten zur Verwirklichung von § 202a StGB weiterzugeben, macht die Präventivfunktion des § 202c StGB also Sinn, da der Vorfeldtäter andernfalls gänzlich straflos bliebe.[159] Zwar bliebe auch ein den § 202a StGB lediglich versuchender Täter ohne den § 202c StGB straflos, doch ist dieser Fall aufgrund der beabsichtigten Straflosigkeit des Versuchs bei § 202a StGB offensichtlich gesetzgeberisch gewollt.

Zweitens wird angemerkt, dass es sich bei dem Vorfelddelikt des § 202c StGB um ein Offizialdelikt handele, das von Amts wegen verfolgt wird, während die Schädigungsdelikte der §§ 202a und 202b StGB als relative Antragsdelikte grundsätzlich eines Strafantrags eines Verletzten bedürfen.[160] Zwar mag es auf den ersten Blick seltsam wirken, dass mit steigender Rechtsgutsbeeinträchtigung die Anforderungen an die Verfolgbarkeit steigen, allerdings ist diese vermeintliche Ungereimtheit tatsächlich wohl lediglich darauf zurückzuführen, dass es beim Vorfelddelikt des § 202c StGB logischerweise noch keinen Verletzten gibt, der einen Strafantrag stellen könnte.[161]

Drittens stellt die Strafbarkeit der Vorbereitung eines Computerbetrugs nach § 263a Abs. 3 StGB einen strafrechtlichen Systembruch dar. Analog zum Betrugstatbestand nach § 263 StGB schützt auch der Computerbetrug das Rechtsgut Vermögen.[162] Das danebenstehende Allgemeininteresse an funktionstüchtigen Datenverarbeitungssystemen in Wirtschaft und Verwaltung wird lediglich mittelbar geschützt.[163] Nun aber weitet § 263a Abs. 3 StGB die Strafbarkeit erheblich aus, indem bereits Handlungen strafrechtlich relevant werden, die deutlich vor einer Rechtsgutbeeinträchtigung angesiedelt sind. Es ist nicht einsichtig, warum der Vermögensschutz, anders als beim regulären Betrug nach § 263

---

159 *Eisele*, Computer- und Medienstrafrecht, § 9 Rn. 61.

160 *Gröseling/Höfinger*, MMR 2007, 626 (628); *Schumann*, NStZ 2007, 675 (680).

161 In diese Richtung argumentierend wohl auch *Ernst*, NJW 2007, 2661 (2664); *Hilgendorf/Valerius*, Computer- und Internetstrafrecht, § 3 Rn. 573.

162 BGHSt 40, 331, 334; *Schmidt*, in: Beck-OK StGB, Stand: 1.12.2016, § 263a Rn. 1; *Perron*, in: Schönke/Schröder (Hrsg.), § 263a StGB Rn 1.

163 *Fischer*, StGB, § 263a Rn 2; *Kindhäuser*, in: NK-StGB Bd. 3, § 263a Rn 2; ablehnend gegenüber auch nur einem mittelbaren Schutz *Lackner/Kühl*, StGB, § 263a Rn. 1.

StGB, hier vorverlagert sein sollte.[164] Nicht nur der Umstand, dass die Einführung eines Computerbetrugstatbestands in das StGB maßgeblich darauf zurückging, dass die Fähigkeit zum Irren i.S.d. § 263 StGB Menschen vorbehalten ist[165] und damit vermögenswirksame Einwirkungen auf Computerprogramme regelmäßig straflos blieben,[166] spricht dafür, eine enge Koppelung der beiden Tatbestände aufrechtzuerhalten. Auch die mittlerweile herrschende Auffassung, dass die Tatbestandsmerkmale des § 263a StGB unter Berücksichtigung der Strukturverwandtschaft zum Betrugstatbestand auszulegen seien,[167] deutet in diese Richtung.

Gesetzessystematische Gesichtspunkte stellen somit einen wichtigen Teil der Kritik an der computerstrafrechtlichen Vorfeldkriminalisierung dar. Der Grundsatz der Straflosigkeit von Vorbereitungshandlungen wirft allerdings noch andere Fragen auf, die im Folgenden umfassend behandelt werden.

C. Verfassungsrecht und computerstrafrechtliche Vorfeldtatbestände

Die oben aufgeführten Vorbereitungsstrafbarkeiten bezeichnen Ausnahmefälle im System des Strafgesetzbuchs und rechtfertigen sich nach herrschender und auch hier vertretener Auffassung in der Regel durch die besondere Schwere der drohenden Rechtsgutsbeeinträchtigung oder die herausgehobene Schutzwürdigkeit eines bestimmten Rechtsguts.[168] Diese gesetzliche Ausnahmestellung spiegelt sich auch in den regelmäßig sehr hohen Strafandrohungen wider.[169] Obwohl durchaus gewichtige Argumente gänzlich gegen die Legitimität einer Strafbarkeit von Vorbereitungshandlungen sprechen,[170] wird im Folgenden die gefestigte Rechtsprechung des Bundesverfassungsgerichts und die herrschende Auffassung zugrunde gelegt, um die computerstrafrechtlichen Vorfelddelikte auf ihre Verfassungsmäßigkeit hin zu überprüfen.

---

164 *Lackner/Kühl*, StGB, § 263a Rn. 26a.

165 Statt aller: *Wohlers/Mühlbauer*, in: MüKo-StGB Bd. 5, § 263a Rn. 1 m.w.N.

166 Vgl. BGH NStZ 2005, 213.

167 BGHSt 47, 160; *Hoyer*, in: SK-StGB Bd. 4, 142. EL Mai 2014, § 263a Rn. 6; *Kindhäuser*, in: NK-StGB Bd. 3, § 263a Rn. 5 f.; so auch bereits der Gesetzgeber im Rahmen der damaligen Gesetzesbegründung; vgl. BT-Drs. 10/5058, 30.

168 Siehe oben, Kap. 3 § 12 A.

169 Zumeist werden Freiheitsstrafen von bis zu fünf oder sogar zehn Jahren bereits für die Verwirklichung des Vorbereitungsdelikts angedroht. Siehe etwa die §§ 89, 89a StGB. § 80 StGB enthält gar eine Strafandrohung von lebenslanger oder mindestens zehnjähriger Freiheitsstrafe.

170 Zur Grundsatzkritik siehe z.B. *Beck*, Vorfeldkriminalisierung, 1992, S. 78 ff; *Jakobs*, ZStW, 97 (1985), 751 ff.; *Zaczyk*, in: NK-StGB Bd. 1, § 22 Rn. 3.

Während die Vorbereitung eines Computerbetrugs nach § 263a Abs. 3 StGB immerhin noch mit einer Strafandrohung von bis zu drei Jahren Freiheitsentzug versehen ist, wartet § 202c StGB lediglich noch mit einem Strafmaß von bis zu einem Jahr Freiheitsstrafe auf.[171] Dass die Gesetzesbegründung die Notwendigkeit der Vorschrift mit dem Ziel, „bestimmte besonders gefährliche Vorbereitungshandlungen" zu kriminalisieren, angibt,[172] mutet bei einer solch geringen Strafandrohung durchaus seltsam an.[173] Den grundsätzlichen Verzicht auf einen frühzeitigen Eintritt der Strafbarkeit mahnt auch der Rat der Europäischen Union in seinen Leitlinien für das Strafrecht der EU an.[174] *Popp* ordnet diesen Bereich des Computerstrafrechts daher auch folgerichtig eher einem „modernen, abstrakten Gefahren und schlechten Absichten nachspürenden Präventionsstrafrecht" zu.[175] *Chou* wird noch deutlicher und bezeichnet § 202c StGB als „Ausdruck eines polizeirechtlichen Denkens und somit mit einem rechtstaatlichen Strafrecht unvereinbar".[176] Die Existenz der Norm beruht ihr zufolge lediglich auf der Annahme, dass der Täter selbst oder andere spätere Inhaber eines solchen Computerprogramms höchstwahrscheinlich Straftaten nach den §§ 202a und 202b StGB begehen werden. Der freiheitliche Abwägungsprozess eines jeden Bürgers über den zukünftigen, legalen oder illegalen, Umgang mit einem Gegenstand werde in diesem Fall also durch eine gesetzgeberische Vorverurteilung ersetzt. Bereits die Willensentschließungsfreiheit einer Person in Kombination mit dem Vorhandensein eines potenziellen Tatwerkzeugs schätzt der Gesetzgeber somit als abstrakte Gefahr hinsichtlich einer Deliktsverwirklichung ein.[177] *Puschke* prägt für diesen strafrechtlichen Ansatz daher auch den Begriff des Interventionsstrafrechts, das nicht mehr in erster Linie zu bestrafen,

---

[171] Folgerichtig geht somit auch etwa *Kochheim*, Cybercrime und Strafrecht, Kap. 1 Rn. 58 davon aus, dass die genannten Vorbereitungsstraftaten dem Bereich der leichten Kriminalität zuzuordnen sind.

[172] BT-Drs. 16/3656, S. 11.

[173] So auch *Schultz*, DuD 2006, 778 (782); *Schumann*, NStZ 2007, 675 (679).

[174] Rat der Europäischen Union, Vermerk v. 27.11.2009, 16542/2/09 REV 2 JAI 868 DROIPEN 160, S. 5: „Die Strafrechtsbestimmungen sollten vorrangig auf Handlungen ausgerichtet werden, die einen tatsächlichen Schaden verursachen oder die die zu schützenden Rechte oder wesentlichen Interessen ernsthaft gefährden; es gilt folglich zu vermeiden, dass eine Handlung unverhältnismäßig früh unter Strafe gestellt wird. Handlungen, die lediglich eine abstrakte Gefahr für die zu schützenden Rechte oder Interessen implizieren, sollten nur dann unter Strafe gestellt werden, wenn die besondere Bedeutung dieser Rechte und Interessen dies rechtfertigt." Abrufbar unter: http://db.eurocrim.org/db/de/doc/1651.pdf (Stand: 21.3.2017).

[175] *Popp*, GA 2008, 375 (393).

[176] *Chou*, Vorbereitungsdelikte, S. 207.

[177] Vgl. dazu *Zaczyk*, in: NK-StGB Bd. 3, § 303a Rn. 17.

sondern zu verhindern, also zu intervenieren versucht, bevor es überhaupt zu Gefährdungen oder Schädigungen kommen kann.[178]

Auch bei § 263a Abs. 3 StGB (Vorbereitung eines Computerbetrugs) sind weitere Bedenken angezeigt, obgleich zumindest die Strafandrohung, wie gezeigt, über den Bagatellbereich hinausreicht. Das geschützte Rechtsgut Vermögen ist wohl anders als das Leben oder der Staat nicht als besonders wertvoll zu klassifizieren[179] und auch ein besonders hoher Gefährlichkeitsgrad der Verhaltensweise bei der Vorbereitung eines Computerbetrugs[180] darf bezweifelt werden. Wie bereits gezeigt, wird die Regelung daher für systembrüchig[181] oder teilweise gar für verfassungswidrig gehalten.[182]

Diesen Ansichten ist zuzustimmen. Es kommt durch die bloße Vorbereitung zur Tat noch nicht zu einer Rechtsverletzung. Zwar ist das auch bei (abstrakten) Gefährdungsdelikten regelmäßig der Fall, allerdings bergen diese bereits eine sog. spezifische Unrechtsqualität in sich.[183] Damit ist gemeint, dass bei abstrakten Gefährdungsdelikten regelmäßig kein weiteres Volldelikt[184] verwirklicht werden kann, sondern der Gefährdungseintritt bereits selbst als solches zu qualifizieren ist.[185]

Beispiel: Die Trunkenheit im Verkehr nach § 316 StGB dient nicht der Vorbereitung zur Verwirklichung einer Körperverletzung mit Todesfolge oder einer Sachbeschädigung. Es wird also nicht die „Vorbereitung zu einer Körperverletzung mit Todesfolge durch betrunkenes Autofahren" bestraft, sondern ein spezifisches Verhalten als per se gefährlich definiert und nicht vom Vorsatz hinsichtlich der Verwirklichung eines Volldelikts abhängig gemacht.

Die Vorbereitung des Ausspähens von Daten durch Herstellung eines dafür geeigneten und bestimmten Computerprogramms nach §§ 202a Abs. 1 i. V. m. 202c Abs. 1 Nr. 2 StGB hingegen bezieht sich unmittelbar auf ein später möglicherweise zu verwirklichendes Volldelikt (nämlich § 202a StGB).

Diese Differenzierung ist auch gerechtfertigt. Bei abstrakten Gefährdungsdelikten liegt die Unrechtsqualität des Verhaltens in der Unbeherrschbarkeit des an-

---

[178] *Puschke*, in Hefendehl (Hrsg.), Grenzenlose Vorverlagerung, S. 9 (25 f.).

[179] *Chou*, Vorbereitungsdelikte, S. 209 m. w. N.

[180] So aber *Duttge*, in: FS Weber (2004), S. 285 (303).

[181] *Husemann*, NJW 2004, 104 (107).

[182] *Duttge*, in: FS Weber (2004), S. 285 (287 ff.); den zugrunde liegenden EU-Rahmenbeschluss hält er gleichzeitig für unverhältnismäßig und damit für unanwendbar.

[183] Vgl. *Köhler*, Strafrecht AT, S. 466.

[184] Durch den Begriff „Volldelikt" soll zum Ausdruck gebracht werden, dass eine Vorbereitungshandlung lediglich ein Zwischenstadium zu weiteren Verwirklichungsstufen in Richtung der Bezugstat darstellt.

[185] Vgl. *Jakobs*, ZStW 97 (1985), 751 (769).

schließenden Geschehens, womit sich eine Strafwürdigkeit begründen lässt. Bei Vorfelddelikten hingegen kann das Geschehen zwischen Vorbereitungs- und Schädigungshandlung vom Täter beherrscht und ggf. in eine andere, das schützenswerte Rechtsgut verschonende Richtung gelenkt werden. Obwohl Vorbereitungsdelikte regelmäßig als Unterkategorie der abstrakten Gefährdungsdelikte angesehen werden, kann hier auch nicht mit der unkontrollierbaren Gefahr argumentiert werden, die ein Täter durch seine tatbestandliche Handlung schafft. Denn bei den computerstrafrechtlichen Vorbereitungsdelikten ist für die volldeliktische Verwirklichung der jeweiligen Bezugstat uneingeschränkt eine weitere Willensmanifestation des Vorfeldtäters erforderlich. Den Geschehensablauf hinsichtlich der Bezugstat hat er durch die Vorfeldtat jedenfalls nicht aus der Hand gegeben.[186]

Ausnahmen vom Grundsatz, strafrechtlich relevantes Verhalten erst bei tatsächlichen Gefährdungen für ein schützenswertes Rechtsgut anzunehmen, sind zwar denkbar, haben jedoch, wie gezeigt, zumindest auf den Schutz besonders wichtiger kollektiver und individueller Rechtsgüter, wie den Bestand des Staats und seiner Einrichtungen oder das Leben, beschränkt zu bleiben. Grundsätzlich rechtlich neutrale Handlungen, wie das Herstellen eines Computerprogramms, die lediglich auf der Basis von Empirie als potenziell gefährlich eingeordnet werden können,[187] verdienen somit keine *strafrechtliche* Intervention, da die benannten verfassungsrechtlichen Voraussetzungen zur Legitimität von Vorbereitungsstrafbarkeiten vorliegend nicht erfüllt sind.

Bereits vor fast 200 Jahren formulierte *Zachariä* dazu eindrucksvoll:

„Der Richter würde gegen Jeden, der in eine Apotheke tritt und Gift fordert, gegen Jeden, der sich ein Gewehr kauft oder Leitern und Stricke angeschafft hat, zu inquirieren berechtigt seyn, ob dies nicht in der Absicht geschehen sey, ein Verbrechen zu verüben, und in tausend anderen Fällen auf eine empörende Weise in das Leben der Bürger eingreifen können. Wer freilich den Staat für ein Sittlichkeit erzwingendes Zuchthaus hält und gewissermaßen bedauert, daß nicht jeder Mensch einen seine Gedanken wiedergebenden und festhaltenden Spiegel auf der Brust hat, um jeden unsittlichen Gedanken erkennbar zu machen und demgemäß strafen zu können, der wird auch Gefallen daran finden, jedes mögliche Indizium des

---

186 So auch *Heinrich*, ZStW 121 (2009), 94 (125).

187 *Hefendehl*, in ders. (Hrsg.), Grenzenlose Vorverlagerung, S. 89 (103) stellt eine solche empirische Absicherung für das Vorbereitungsdelikt des Herstellens einer Geldfälschungsmaschine nach § 149 StGB infrage. Ähnlich verhält es sich mit den Vorbereitungsdelikten des Computerstrafrechts. Auch wenn es psychologisch einleuchtend erscheint, dass der Hacker sein Programm zu einem späteren Zeitpunkt zur Tatbestandverwirklichung einsetzt, ist weder die „echte“ noch die „vermutete“ Empirie ausreichend, um bereits die Herstellung des Programms unter Strafe zu stellen. Auch *Paeffgen*, in: FS Amelung (2009), S. 81 (115), bleibt bezüglich der Vorfelddelikte unter Heranziehung von Empirie kritisch, obgleich er sie nicht grundsätzlich ausschließen will, solange sowohl ein Rechtsgutsbezug und materialisierbares Handlungsunrecht gegeben sind.

verbrecherischen Willens für strafbaren Versuch zu erklären. Hoffentlich werden aber solche Principien nie positive Anwendung finden!"[188]

Dem ist auch im Hinblick auf das Computerstrafrecht nichts hinzuzufügen. Selbstverständlich kann eine Rechtsgemeinschaft bereits in diesem Stadium mit rechtlich relevanten Maßnahmen auf ein Verhalten, das sie als gefährlich und Schaden bringend einordnet, reagieren; ein strafrechtliches Unwerturteil sollte jedoch schlechterdings nicht dazu gehören. Die *Ultima-Ratio*-Funktion des Strafrechts gebietet die Ausschöpfung sämtlicher zur Verfügung stehenden weniger eingriffsintensiven Maßnahmen, bevor die Mittel der strafrechtlichen Kriminalisierung und Strafandrohung zur Anwendung kommen. Grundsätzlich stehen dazu mindestens zivilrechtliche Ahndungsmethoden und gefahrenabwehrrechtliche Maßnahmen des Polizei- und Ordnungsrechts zur Verfügung.[189]

Im folgenden Abschnitt wird daher dreierlei untersucht: erstens, ob es sich bei den computerstrafrechtlichen Vorfelddelikten nicht eigentlich um gefahrenabwehrrechtliche Maßnahmen handelt[190] und welche Konsequenzen sich aus einer solchen Feststellung, insbesondere hinsichtlich der EU-Kompetenzmäßigkeit der Richtlinie 2013/40/EU, ergäben.[191] Zweitens, ob materielle Grenzen bei der Kompetenzausübung, namentlich die nationalen Identitäten nach Art. 4 Abs. 2 S. 1 EUV, hinreichend beachtet worden sind.[192] Und schließlich drittens, ob das desintegrativ oder auch souveränitätsschonend angelegte Instrument des strafrechtlichen Notbremsemechanismus nach Art. 83 Abs. 3 AEUV hinsichtlich der Richtlinie 2013/40/EU von Deutschland hätte ausgelöst werden können.[193]

D. Untersuchung der (Teil-)Nichtigkeit von Richtlinie 2013/40/EU

Während sich das Strafrecht und die Strafverfolgungsorgane schwerpunktmäßig mit repressiven Mitteln eines Sachverhalts annehmen, ist präventives Vorgehen in Gefährdungssituationen maßgeblich den Polizei- und Ordnungsbehörden vorbehalten. Letztere nehmen zwar zusätzlich auch repressiv-strafrechtliche

[188] *Zachariä*, Die Lehre vom Versuche der Verbrechen, 1. Theil, S. 210.

[189] Siehe etwa *Ashworth/Horder*, Criminal Law, S. 33.

[190] Auch *Sieber*, NStZ 2009, 353 (356 f.), geht – dort allerdings bezüglich der Vorbereitungshandlungen im Terrorismusstrafrecht – der Frage nach, wann präventive Maßnahmen nicht mehr dem Strafrecht, sondern vielmehr dem Gefahrenabwehrrecht oder einem hybriden Sicherheitsrecht zuzuordnen sind und welche Konsequenzen sich aus derartigen Einordnungen ergeben könnten.

[191] Kap. 3 § 12 D. I.

[192] Kap. 3 § 12 D. II.

[193] Kap. 3 § 12 D. II. 2.

Aufgaben wahr, dann jedoch regelmäßig als sog. Ermittlungspersonen der Staatsanwaltschaft gem. § 152 Abs. 1 GVG. Anders ausgedrückt, ist die Verhinderung zukünftiger Normverstöße dem polizeilichen Aufgabenbereich zugeordnet und nicht Sache des Strafrechts.[194]

Polizeiliches Handeln zeichnet sich unter anderem dadurch aus, dass nicht erst gesichertes Wissen und Beweise, sondern bereits Verdachtsmomente unterschiedlicher Intensität Eingriffsbefugnisse verleihen. Bei strafrechtlich relevanten Vorbereitungshandlungen begegnet man regelmäßig einer ähnlichen Konstellation. Die angeblich strafwürdige Verhaltensweise ist nicht erwiesenermaßen schädlich oder gefährlich für schützenswerte Rechtsgüter, sondern bietet lediglich gewisse Anhaltspunkte, um auf eine später folgende Rechtsgutsgefährdung oder -schädigung zu schließen.

Wie bereits gezeigt, deuten die sehr niedrigen Strafandrohungen bei den computerstrafrechtlichen Vorfelddelikten nicht auf eine besondere Gefährlichkeit des Verhaltens hin und auch die potenziell zu einem späteren Zeitpunkt betroffenen Rechtsgüter[195] sind im Vergleich zu denen anderer Vorfelddelikte nicht als hochwertig einzustufen.[196] Anstatt also polizeiliches Denken in den strafrechtlichen Maßnahmenkatalog aufzunehmen und dadurch die ohnehin verfassungsrechtlich und systematisch fragwürdige Kriminalisierung von Vorbereitungshandlungen auf minderschwere Delikte der Computerkriminalität auszuweiten, wäre vielmehr vorrangig ein polizeirechtlicher Umgang mit den Vorfeldhandlungen zu den §§ 202a, 202b, 263a Abs. 1, 303a und 303b StGB geboten.

Sollten empirische oder gar tatsächliche Anhaltspunkte darauf hindeuten, dass bestimmte Handlungen typischerweise den genannten Straftaten vorangehen, sind ordnungsrechtliche Gegenmaßnahmen durchaus gerechtfertigt und gegebenenfalls sogar geboten bzw. notwendig. Auch wenn etwa das Mitsichführen eines Baseballschlägers auf einer Demonstration nicht strafrechtlich relevant ist, können die zuständigen Ordnungsbehörden dies selbstverständlich untersagen, die Einhaltung der Untersagung kontrollieren und schließlich nötigenfalls auch durchzusetzen. Zur Verhinderung der Herstellung von Program-

---

[194] *Jakobs*, Staatliche Strafe, S. 31.

[195] Die ganz h. M. geht davon aus, dass die Rechtsgüter der computerstrafrechtlichen Vorbereitungsdelikte diejenigen sind, die auch von den Vollendungstatbeständen geschützt werden sollen: siehe dazu exemplarisch *Graf*, in: MüKo-StGB Bd. 4,§ 202c Rn. 2 und *Perron*, in: Schönke/Schröder (Hrsg.), § 263a StGB Rn. 1.

[196] § 80 StGB schützt die Sicherheit Deutschlands; siehe etwa *Classen*, in: MüKo-StGB, § 80 Rn. 1; § 89a StGB schützt das Leben sowie den Bestand und die Sicherheit des Staats; siehe etwa *Lackner/Kühl*, StGB, § 89a Rn. 2; §§ 202c, 202a StGB schützen hingegen lediglich formelle Verfügungsbefugnis des Inhabers der Daten; siehe etwa *Gercke, M.*, in: Spindler/Schuster (Hrsg.), Recht der elektronischen Medien, § 202a Rn. 1.

men, die zur Begehung der o. g. Computerstraftaten geeignet und bestimmt sind, wäre analog beispielsweise ein Verbot der Herstellung von und des Handels mit derartigen Programmen denkbar. Zudem kämen auch Überwachungen und Überprüfungen von identifizierten Gefährdern in Betracht, wie es offline etwa bei der sog. Hooligan-Szene üblich ist. Auch die polizeiliche Registrierung von IT-Sicherheitsexperten, die auf den Umgang mit potenziell gefährlicher und auch zur Begehung von Straftaten geeigneter Software angewiesen sind, wäre denkbar. So könnten einerseits staatliche Stellen den Überblick hinsichtlich des Umgangs mit Schadprogrammen behalten und andererseits gleichzeitig vermieden werden, dass das technisch, unternehmerisch und gesellschaftlich relevante und gewünschte Verhalten dieser Berufsgruppe mit strafrechtlicher Indizwirkung belegt würde. In diese Richtung gehende Ansätze lassen sich aktuell zum Beispiel in der Ausweitung einer sog. Online-Streife erkennen, die sich derzeitig freilich vor allem auf die Aktivitäten in den sozialen Netzwerken konzentriert.[197] Entsprechend sind aber auch Online-Ermittlungen und polizeiliche Recherchen im sog. Deep- sowie Darknet denkbar, um potenzielle Gefahren frühzeitig zu erkennen und diesen entgegenzutreten.[198] Selbstverständlich stellen sich bei solchen polizei- und ordnungsrechtlichen Ermittlungsmethoden eigene verfassungsrechtliche Fragen. Ein Ausweichen auf das schärfste Schwert des Rechtsstaats, das Strafrecht, bietet u. a. durch das explizite Unwerturteil über ein Verhalten jedoch eine deutlich stärkere Eingriffsintensität, wie noch zu zeigen sein wird.[199]

Die Richtlinie ist allerdings dahin gehend eindeutig, dass in den Fällen der genannten Vorbereitungsdelikte eine *Strafbarkeit* mit konkreten Mindest-Höchststrafen gefordert wird. Zur Umsetzung dieser Vorgaben war und ist Deutschland unionsrechtlich verpflichtet. Insbesondere die gleichzeitige Verknüpfung der Vorfeldstrafbarkeiten mit konkreten Anforderungen an Strafen lässt einer mitgliedstaatlichen Umsetzung im Rahmen des Polizeirechts demgemäß keinen Raum.

---

[197] Zur Verfassungsmäßigkeit dieses polizeilichen Instruments siehe *Oermann/Staben*, Der Staat 2013, 630 ff.

[198] Vielversprechende Ansätze lassen sich beispielsweise bei Interpol erkennen, das seit Juli/August 2015 Polizisten aus verschiedenen Ländern für die Ermittlungstätigkeit im Darknet ausbildet; siehe dazu http://www.interpol.int/News-and-media/News/2015/N2015-108 (Stand: 07.08.2017). Auch das MEMEX-Programm unter Beteiligung der NASA zur Ermöglichung einer Durchsuchung des Dark- sowie Deepnets bietet den Ordnungsbehörden neue Möglichkeiten zur Aufdeckung und gegebenenfalls Verhinderung geplanter Straftaten im Internet; abrufbar unter: http://memex.jpl.nasa.gov (Stand: 07.08.2017).

[199] Siehe unten, Kap. 3 § 12 D. I. 1. a.

Anders wäre es etwa, wenn die Richtlinie nicht die Gewährleistung der Bestrafung mit einer konkreten Strafhöhe (Freiheits- und Geldstrafe), sondern z. B. lediglich „ein strafrechtliches Vorgehen" gegen die Vorbereitung eines rechtswidrigen Systemeingriffs fordern würde. Dann wäre es ggf. denkbar, durch eine weite Auslegung des EU-rechtlichen Strafbarkeitsbegriffs auch polizei- und ordnungsrechtliche Maßnahmen genügen zu lassen – insbesondere mit dem Argument, dass die strikte Trennung von präventivem Gefahrenabwehrrecht und repressivem Strafrecht nicht in allen mitgliedstaatlichen Rechtsordnungen konsequent verankert ist,[200] *sodass etwa Deutschland auch mit gefahrenabwehrrechtlichen Mitteln den „Strafbarkeitsverpflichtungen" der EU-Richtlinie nachkommen könnte.*

Wie noch zu zeigen sein wird,[201] verlangt die Richtlinie 2013/40/EU von den Mitgliedstaaten gleichwohl eine derart weitgehende Kriminalisierung von Vorbereitungshandlungen, dass eine Vereinbarkeit mit verfassungsrechtlichen Grundprinzipien kaum anzunehmen ist.[202] Eine Reduktion der Richtlinien-Anforderungen auf einen verfassungsgemäßen Kernbereich bzw. eine geltungserhaltene Interpretation der Richtlinie im Wege der Umdeutung der Vorbereitung*sstrafbarkeit* zu *allgemeinen präventiv-rechtlichen Maßnahmen* ist unter Wahrung des Vorrangs des EU-Rechts ebenfalls nicht möglich. Durch die „Verpolizeirechtlichung des Strafrechts" entsteht mithin ein Konflikt zwischen nationalem Verfassungsrecht und Unionsrecht.[203]

Es ist allerdings denkbar, dass die Auflösung dieses Konflikts bereits aus dem Unionsrecht selbst heraus möglich ist. Jenes hat nämlich eigenständige Mechanismen, um die Verfassungsgrundsätze der Mitgliedstaaten bei der Unionsgesetzgebung angemessen zu berücksichtigen.[204] Möglicherweise könnte daher die Vorgabe, computerstrafrechtliche Vorfelddelikte in nationales Strafrecht zu implementieren, bereits die unionsrechtliche (Teil-)Nichtigkeit der Richtlinie nach sich ziehen. Im Folgenden wird deshalb untersucht, ob die Anordnung zur

---

[200] Dazu sogleich, Kap. 3 § 12 D. I. 1.

[201] Siehe unten, Kap. 3 § 12 D. I.

[202] Freilich ist das Unionsrecht grundsätzlich dem mitgliedstaatlichen (Verfassungs-) Recht vorrangig, sodass abgesehen von Ausnahmefällen diese Vereinbarkeit nicht Voraussetzung einer rechtmäßigen EU-Richtlinie ist. Unabhängig davon greift auch der deutsche Strafgesetzgeber ohnehin vermehrt auf das Strafrecht zur Gewährleistung von Sicherheit zurück (siehe dazu *Bäcker*, Kriminalpräventionsrecht, S. 331 ff.), sodass zumindest aus politischen Gründen dieser Konflikt zwischen deutschem Verfassungsrecht und Unionsrecht von nationaler Seite regelmäßig gar nicht erkannt wird; siehe *Folz*, ZIS 2009, 427 (430).

[203] Auch *Hahn-Lorber*, EJR 2010, 760 (763 f.), weist darauf hin, dass derartige Konflikte durch einander im Mehrebenensystem überlagernde Rechtsordnungen unausweichlich sind.

[204] Beispielhaft sei hier lediglich die Identitätsklausel des Art. 4 Abs. 2 EUV genannt; dazu vgl. im Einzelnen Kap. 3 § 12 D. II. 1.

Implementierung von Vorbereitungsstrafbarkeiten im Computerstrafrecht möglicherweise gegen EU-Recht verstößt.

Die (Teil-)Nichtigkeit der Richtlinie könnte sich vorliegend aus der Unzuständigkeit, der Verletzung wesentlicher Formvorschriften und der Verletzung des Vertrags oder einer bei seiner Durchführung anzuwendenden Rechtsnorm gem. Art. 263 Abs. 2 AEUV ergeben. Um eine allgemeine Auseinandersetzung mit der Nichtigkeitsklage und den mit diesem Rechtsschutzmittel verbundenen Herausforderungen zu vermeiden und eine Fokussierung auf die relevanten Gesichtspunkte einer potenziellen Nichtigkeit der Richtlinie zu ermöglichen, konzentriert sich die folgende Untersuchung auf die Aspekte der Begründetheit und dabei insbesondere auf die Kompetenzmäßigkeit des EU-Rechtsakts[205] und dessen Vereinbarkeit mit weiteren Primärrechtsnormen des AEUV[206].

I. Kompetenzmäßigkeit

Fraglich ist zunächst, ob Art. 83 Abs. 1 AEUV überhaupt einen tauglichen Kompetenztitel bereitstellt. Für die Harmonisierung des mitgliedstaatlichen Computerstrafrechts wird man das annehmen können. Weniger eindeutig ist jedoch die Zuordnung der fraglichen Tatbestände mit Vorbereitungscharakter zum strafrechtlichen Regelungsbereich. Die Entscheidung hängt dabei ganz grundsätzlich von der Frage ab, ob und wie man eine Grenzziehung zwischen dem Bereich des Strafrechts und dem des Gefahrenabwehrrechts vornimmt. Möglicherweise kommt man dann zu der Einschätzung, dass zwar strafrechtliche Termini verwendet und strafrechtstypische Rechtsfolgen angeordnet, aber gleichwohl Regelungsmaterien adressiert werden, die bei genauerer Betrachtung lediglich scheinbar dem Strafrecht zuzuordnen sind.[207]

Dabei ist zunächst zweierlei zu beachten: Einerseits ist im Hinblick auf die autonome Ausgestaltung der EU-Rechtsordnung einer EU-rechtlichen Definition des Strafrechtsbegriffs zu folgen. Andererseits kann die Rechtsauffassung der EU-Institutionen hinsichtlich einer Qualifizierung von Normen als „strafrechtlich" nicht allein entscheidend sein. Die autonome Begriffsbestimmungs- und Auslegungshoheit des EuGH bezüglich des EU-Rechts ist zwar ihrem Grunde nach unbestritten, unterliegt allerdings dennoch interpretatorischen Einschränkungen und Präzisierungen. Insbesondere wenn der Wortlaut einer Norm nicht eindeutig ist, sind neben systematischen und teleologischen auch

---

[205] Kap. 3 § 12 D. I.

[206] Kap. 3 § 12 D. II.

[207] Vgl. *Beck*, Vorfeldkriminalisierung, S. 97, der vor allem für die politischen Vorfeldtatbestände aufzeigt, dass oftmals lediglich durch die Verwendung strafrechtlicher Begriffe neutrales Verhalten umetikettiert wird.

rechtsvergleichende Erwägungen heranzuziehen. Vor allem der Grundsatz einer gleichrangigen Vielsprachigkeit des Unionsrechts führt dazu, dass eine ausschließlich grammatische Auslegung von EU-rechtlichen Normen lediglich in Ausnahmefällen zielführend sein kann. Der (verfassungs-)gerichtliche Dialog[208] als Umsetzung der Art. 19 EUV, Art. 6 Abs. 3 EUV und Art. 340 Abs. 2 EUV ist damit oftmals notwendiger Bestandteil eines Auslegungsvorgangs und wirkt sich nicht lediglich im Rahmen rechtsvergleichender, sondern gleichermaßen auch bei systematischen und teleologischen Erwägungen aus.[209] Eine vollständige Autonomie des EU-Rechts bei der Auslegung von Rechtsbegriffen, die in den Rechtssystemen aller oder zumindest einiger Mitgliedstaaten traditionell bereits einen bestimmten Bedeutungsgehalt gewonnen haben, ist demnach regelmäßig nicht möglich. Ansonsten läge keine interpretatorische Lückenfüllung unter Berücksichtigung mitgliedstaatlicher Verfassungswerte vor.[210] Stattdessen würden die EU-Institutionen die Möglichkeit erhalten, durch losgelöste Begriffsbestimmungen im Kompetenzrecht die sog. Kompetenz-Kompetenz „durch die Hintertür" einzuführen. Faktisch wäre eine Bestimmung des Kompetenzbereichs der EU dann gar nicht mehr sinnvoll möglich, da die Union selbst entschiede, wie weit oder eng die einzelnen Kompetenzen, in diesem Fall die Kriminalitätsbereiche, gehen.[211]

Auch wenn es sich beim EU-Recht um eine autonome Rechtsordnung mit eigener Interpretationsmethodik handelt und der Wille der Vertragspartner nicht allein ausschlaggebend ist, sondern dynamische Entwicklungen in den Auslegungsvorgang einfließen, sind diesem Prozess daher dennoch gewisse Grenzen zu setzen. Wenn Begrifflichkeiten und damit einhergehend Kompetenzen durch die EU-Organe ohne Rücksicht auf die Auslegungspraxis der mitgliedstaatlichen (Verfassungs-)Gerichte interpretiert würden, käme dies einer Kompetenz-Kompetenz gleich, was durch Art. 5 Abs. 1 und 2 EUV explizit ausgeschlossen ist.

Zur Verdeutlichung folgendes (überzeichnetes) Beispiel: Die Vertragspartner, also die Mitgliedstaaten der Europäischen Union, einigen sich auf eine Änderung des EU-Primärrechts dahin gehend, dass eine Kompetenzübertragung vom nationalstaatlichen Bereich auf die EU für die Harmonisierung des Lebens-

---

[208] Siehe bereits oben, Kap. 2 § 7 C. I. 2. b. cc.

[209] Vgl. *Lenaerts/Gutiérrez-Fons*, EUI Working Paper AEL 2013/09, 3 (47 f.).

[210] Vgl. *Lenaerts/Gutiérrez-Fons*, EUI Working Paper AEL 2013/09, 3 (47).

[211] *Weigend*, ZStW 2004 (116), 275 (285), der explizit auf die Unschärfe des Computerkriminalitätsbegriffs abstellt und vermutet, die Autoren (zum damaligen Zeitpunkt noch der Verfassungskonvent) des Vertrags von Lissabon seien naiverweise davon ausgegangen, dass die Kriminalitätsbereiche des jetzigen Art. 83 Abs. 1 UAbs. 2 StGB eindeutig bestimmt wären.

mittelrechts stattfindet. Die Institutionen der EU erlassen daraufhin Richtlinien zum Energierecht, da nach autonomer EU-rechtlicher Interpretation ohne Energie schließlich kein Leben denkbar wäre und damit energierechtliche Fragestellungen dem Lebensmittelrecht zuzuordnen seien.

Durch nahezu willkürliche Interpretations- und Auslegungsvorgänge bestünde dadurch für die EU im Extremfall die Möglichkeit, eigene neue Kompetenzen zu schaffen, wenn die begriffliche Autonomie unbeschränkt bzw. unbeschränkbar wäre.

Vorliegend hängt von der Interpretation des Strafrechtsbegriffs und seiner Abgrenzung zum Begriff des Gefahrenabwehr- bzw. Ordnungs- oder Polizeirechts[212] ab, ob die EU eine Regelungskompetenz für die fraglichen Normen mit Vorbereitungscharakter hat. Ist eine Maßnahme also als „präventiv-polizei- bzw. gefahrenabwehrrechtlich" oder „repressiv-strafrechtlich" einzuordnen?[213] Beide Rechtsbereiche sind eng miteinander verknüpft und daher auch gemeinsam im Titel V des AEUV, also in den Bestimmungen zum Raum der Freiheit, der Sicherheit und des Rechts nach Art. 67 ff. AEUV, verankert. Durch Art. 67 ff. AEUV ist polizei- und gefahrenabwehrrechtliches Handeln, anders als gewisse Bereiche des Strafrechts, explizit im mitgliedstaatlichen Kompetenzbereich belassen. Art. 69 AEUV bringt daher auch zum Ausdruck, dass die Gewährleistung der inneren Sicherheit eine mitgliedstaatliche Schwerpunktaufgabe darstellt.[214] Lediglich die unionale Kooperation und Zusammenarbeit wird von den Kompetenzen des Raumes der Freiheit, der Sicherheit und des Rechts erfasst (siehe Art. 87 AEUV: „Polizeiliche Zusammenarbeit").

Die gefahrenabwehrrechtlichen EU-Kompetenzen statuiert Kapitel 5, Art. 87 ff. AEUV zur polizeilichen Zusammenarbeit. Besondere Bedeutung hat bei der Kompetenzbegrenzung zusätzlich Art. 72 AEUV.[215]

Grundsätzlich sind somit nur die Mitgliedstaaten zur Ergreifung von Maßnahmen in diesem Bereich befugt.[216] Der EU ist im Hinblick auf die Aufrecht-

---

[212] Trotz denkbarer Unterschiede werden die Begriffe im Folgenden synonym verwendet, da es hier ausschließlich auf eine Abgrenzung zum Strafrecht ankommt.

[213] Selbstverständlich erfüllt das Strafrecht neben seiner Repressivfunktion nach ganz h. M. auch präventive Aufgaben. Unter diese Kategorie ist etwa der Abschreckungseffekt einer Strafandrohung zu fassen. Allerdings handelt es sich hierbei nicht um die Verhütung einer Straftat im klassischen Sinne, sondern vielmehr um einen Fall der „Prävention durch Repression"; so *Jescheck/Weigend*, Strafrecht AT, S. 4; *Roxin*, Strafrecht AT Bd. 1, § 3 Rn. 59 ff.

[214] Etwa *Kugelmann*, in: Böse (Hrsg.), EnzEuR Bd. 9, § 17 Rn. 168.

[215] Art. 72 AEUV: „Dieser Titel berührt nicht die Wahrnehmung der Zuständigkeiten der Mitgliedstaaten für die Aufrechterhaltung der öffentlichen Ordnung und den Schutz der inneren Sicherheit."

[216] *Herrnfeld*, in: Schwarze (Hrsg.), Art. 72 AEUV Rn. 1; *Röben*, in: Grabitz/Hilf/Nettesheim (Hrsg.), 57. EL Aug. 2015, Art. 72 AEUV Rn. 16.

erhaltung der öffentlichen Ordnung und den Schutz der inneren Sicherheit normatives Handeln hingegen nicht gestattet.[217] Dies verdeutlicht die besondere Relevanz des Gefahrenabwehrrechts für die Souveränität eines Nationalstaats.[218] Über die in den Abschnitten zur justiziellen und polizeilichen Zusammenarbeit integrierten Kompetenzübertragungen zugunsten der EU ist jene daher nicht berechtigt, Maßnahmen zur Gewährleistung der inneren Sicherheit oder zur Aufrechterhaltung der öffentlichen Ordnung zu ergreifen. Dem Begriff der Maßnahmen unterfallen hierbei sowohl polizeiliche Maßnahmen von Vollzugsbeamten[219] als auch normatives Handeln von EU-Organen.[220] Art. 276 AEUV[221] unterstützt die These einer mangelnden EU-Kompetenz zur Regelung des materiellen Gefahrenabwehrrechts zusätzlich, da ansonsten zwar die Kompetenz für die Harmonisierung des materiellen Rechts auf Seiten der EU bestünde, gleichzeitig aber der EuGH nicht über derartige Maßnahmen judizieren könnte.[222]

Durch die grundsätzliche Zuordnung gefahrenabwehrrechtlicher Maßnahmen zur Domäne der Mitgliedstaaten wird also verdeutlicht, dass dieses von strafrechtlichen Vorgaben des EU-Gesetzgebers abzugrenzen sind. Von teleologischer Warte kommt etwa dem Art. 72 AEUV nur dann eine Bedeutung zu, wenn es auch eine klare Trennung von Strafrecht und Gefahrenabwehrrecht gibt. Wo aber verläuft diese Grenze im Recht der Europäischen Union?

Wie bereits oben ausgeführt,[223] ist innerhalb des Interpretationsvorgangs nicht von einem Stufenverhältnis auszugehen, sondern vielmehr derjenigen Auslegungsmethode der Vorzug zu geben, die den Anforderungen des EU-Rechts am besten gerecht wird. Die Tatsache, dass der AEUV sowohl Regelungen mit strafrechtlichen als auch solche mit ordnungs- und polizeirechtlichen Elementen enthält, lässt in systematischer Hinsicht darauf schließen, dass auch

---

[217] *Rossi*, in: Calliess/Ruffert (Hrsg.), Art. 72 AEUV, Rn. 5; *Weiß*, in: Streinz (Hrsg.), Art. 72 AEUV Rn. 2 jeweils m. w. N.

[218] So auch BVerfGE 49, 24 (56 f.); *Götz*, in: Isensee/Kirchhof (Hrsg.), Handbuch des Staatsrechts Bd. 6, § 85 Rn. 18 ff.

[219] *Weiß*, in: Streinz (Hrsg.), Art. 72 AEUV Rn. 2; derzeitig ist dieser Aspekt mangels ausführender EU-Beamten wohl eher theoretischer Natur.

[220] *Röben*, in: Grabitz/Hilf/Nettesheim (Hrsg.), 57. EL Aug. 2015, Art. 72 AEUV Rn. 13.

[221] „Bei der Ausübung seiner Befugnisse im Rahmen der Bestimmungen des Dritten Teils Titel V Kapitel 4 und 5 über den Raum der Freiheit, der Sicherheit und des Rechts ist der Gerichtshof der Europäischen Union nicht zuständig für die Überprüfung der Gültigkeit oder Verhältnismäßigkeit von Maßnahmen der Polizei oder anderer Strafverfolgungsbehörden eines Mitgliedstaats oder der Wahrnehmung der Zuständigkeiten der Mitgliedstaaten für die Aufrechterhaltung der öffentlichen Ordnung und den Schutz der inneren Sicherheit."

[222] Ähnlich auch *Kugelmann*, in: Böse (Hrsg.), EnzEuR Bd. 9, § 17 Rn. 169.

[223] Siehe oben, Kap. 2 § 7 C. 2. a.

das EU-Recht nicht von einer vollständigen Verschränkung jener Rechtsgebiete ausgeht[224] und daher grundsätzlich eine, wie auch immer geartete, Differenzierung vorzunehmen ist.[225]

1. Rechtsvergleichende Aspekte zur Abgrenzung zwischen Polizeirecht und Strafrecht

Ungeachtet der grundsätzlichen Schwierigkeiten einer grammatischen Auslegung im EU-Recht, die vor allem auf die Vielsprachigkeit der Rechtsmaterie und die Gleichrangigkeit der Vertragssprachen zurückgeht, erscheint eine ausschließlich am Wortlaut orientierte Abgrenzung zwischen Polizeirecht und Strafrecht kaum sinnvoll möglich. Systematische und teleologische Erwägungen unterstützen zwar, wie angedeutet, die Notwendigkeit einer solchen Trennung, bieten selbst jedoch keine hinreichenden Anhaltspunkte für die Manifestation einer EU-rechtlichen Grenzlinie. Diese Leerstelle des EU-Rechts ist demgemäß rechtsvergleichend unter Heranziehung der gemeinsamen verfassungsrechtlichen Traditionen der Mitgliedstaaten auszufüllen.[226] Dabei ist zwar durchaus relevant, wie sich eine Mehrzahl der mitgliedstaatlichen Verfassungstraditionen zu einer bestimmten Fragestellung positioniert, allein ausschlaggebend ist dies jedoch nicht,[227] sodass durchaus auch die Traditionen einer Minderheit unter den Mitgliedstaaten entscheidend sein können. Letztlich ist im Rahmen des EU-rechtlichen Auslegungsvorgangs zu evaluieren, welche mitgliedstaatlichen Ansätze am besten geeignet sind, um die Ziele des EU-Rechts zu verwirklichen.

Vorliegend ist bereits festgestellt worden, dass der AEUV durch die Existenz beider Rechtsbereiche selbst von einer Trennung zwischen Gefahrenabwehrrecht und Strafrecht ausgeht, sodass rechtsvergleichende Aspekte insbesondere aus solchen mitgliedstaatlichen Verfassungstraditionen zu erhalten sind, denen diese Unterscheidung inhärent ist.[228] Damit stellt sich die Frage, welche europä-

---

[224] Grundsätzlich wäre eine solche Konstruktion im Sinne eines gebietsübergreifenden allg. Sicherheitsrechts denkbar. Die Realitäten und Gefahren eines solchen allg. Sicherheitsrechts können hier allerdings nicht weiter thematisiert werden.

[225] *Puschke*, in Hefendehl (Hrsg.), Grenzenlose Vorverlagerung, S. 9 (17 ff.) und *Hefendehl*, in ders. (Hrsg.), Grenzenlose Vorverlagerung, S. 89 (97 f.), gehen allerdings davon aus, dass überstaatliches Recht und ausländische Rechtsordnungen, anders als das deutsche Strafrecht, nicht trennscharf zwischen Repression und Prävention unterscheiden. A. A. *Bäcker*, Kriminalpräventionsrecht, S. 331 ff., der zwar ähnliche Tendenzen erkennt, jedoch nachweist, dass der deutsche Gesetzgeber oftmals über die internationalen Vorgaben hinausgeht und daher eher auf einen europäischen Trend zum präventiven Einsatz des Strafrechts schließt.

[226] Vgl. *Lenaerts/Gutiérrez-Fons*, EUI Working Paper AEL 2013/09, 3 (35) m. w. N.

[227] *Lenaerts/Gutiérrez-Fons*, EUI Working Paper AEL 2013/09, 3 (39) m. w. N.

[228] Im tschechischen Recht etwa findet eine Differenzierung (noch) nicht durchgehend

ischen Rechtsordnungen eine Abgrenzung zwischen diesen Gebieten vornehmen, wie jene ausgestaltet ist und schließlich, ob sich daraus eine europäische Verfassungstradition ableiten lässt bzw. welche der verschiedenen Traditionen dem EU-Recht am besten gerecht wird.

Wie das von der European Criminal Policy-Initiative erarbeitete Manifest zur Europäischen Kriminalpolitik zeigt, sind die strafrechtlichen Verfassungstraditionen der Mitgliedstaaten der EU dem Grunde nach weniger heterogen, als man zunächst annehmen könnte.[229] Alle hier wesentlichen Grundsätze, um Gefahrenabwehrrecht und Strafrecht voneinander abgrenzen zu können, machen die Basis vieler Strafrechtssysteme aus. Unter Beachtung jener Parameter und ausgewählter EU-Rechtssysteme wird die Abgrenzung im Folgenden schwerpunktmäßig anhand der deutschen, französischen und spanischen Verfassungstraditionen nachvollzogen.[230] Insbesondere ist zu überprüfen, ob das deutsche Verständnis flächendeckend innerhalb der Europäischen Union anzutreffen ist oder ob sich ebenfalls fließende Übergänge zwischen Präventiv- und Repressivnormen in mitgliedstaatlichen Strafrechtsordnungen nachweisen lassen.[231]

Obwohl die hier untersuchten Tatbestände des Computerstrafrechts Teil des materiellen Strafrechts sind, behandelt die Abgrenzung zwischen Gefahrenabwehrrecht und Strafrecht vielfach den Grenzbereich polizeilicher und strafprozessualer Eingriffsbefugnisse. Dies ergibt sich aus dem Umstand, dass an dieser Trennlinie regelmäßig Abgrenzungsschwierigkeiten entstehen, wenn etwa zu entscheiden ist, ob in einem konkreten Fall die Ordnungsbehörden oder die

---

statt, sodass oftmals dieselben Normen sowohl für gefahrenabwehrrechtliche als auch für strafrechtliche Maßnahmen herangezogen werden; vgl. dazu *Heid*, Polizeirecht, S. 83 ff.

[229] Die European Criminal Policy-Initiative versammelt 14 Strafrechtsprofessoren aus zehn europäischen Ländern.

[230] Aufgrund der jeweiligen national-rechtlich geprägten Sozialisation eines jeden Rechtswissenschaftlers ist es vielfach gar nicht möglich, einen echten autonomen unionsrechtlichen Auslegungs- und Begründungsvorgang darzustellen. Sprachliche und systematische Divergenzen sind dabei nur eine relevante Schwierigkeit. *Hatje/Mankowski*, EuR 2014, 155 (157, 169) weisen einerseits auf diese gängige und doch oftmals verschwiegene Tatsache hin und machen andererseits deutlich, dass in einem Europa der Vielfalt auch ein national-rechtlich beeinflusstes Unionsrecht systemimmanent und maßgeblicher Baustein des europäischen Normengefüges ist. Daher ist es an dieser Stelle wichtig, den Umstand der deutschen Perspektive der Argumentation nicht zu verschleiern. Vielmehr ist diese vermeintliche Begrenztheit der Argumentation im Unionsrecht sowohl durchaus angelegt als auch unschädlich für das Auslegungsergebnis, da eben auch auf diese Weise dem europäischen Rechtspluralismus Ausdruck verliehen wird.

[231] Da lediglich die Frage zu klären ist, ob die EU bei ihrem Verständnis zumindest auf eine mitgliedstaatliche Strafrechtsordnung verweisen kann, ist eine umfassendere rechtsvergleichende Analyse zur Abgrenzung zwischen Polizeirecht und Strafrecht an dieser Stelle nicht erforderlich.

Strafverfolgungsorgane eines Staats zuständig sind. Diese Konzentration auf den prozessualen Teil des Strafrechts stellt jedoch keine argumentative Hürde dar, da mit einer etwaigen Zuordnung zum strafverfolgungsbehördlichen Kompetenzbereich jeweils eine, zumindest implizite, staatliche Auffassung verdeutlicht wird, es handele sich um die Verfolgung oder Aufklärung einer bereits begangenen und eben gerade nicht um die Verhinderung einer noch bevorstehenden Straftat.[232]

a. Deutsches Recht

Im deutschen Recht erfolgt die Grenzziehung zwischen Polizeirecht und Strafrecht anhand einer Differenzierung zwischen der Entscheidung über die Gefährlichkeit einer Person auf der einen und der Gefährlichkeit (in diesem Fall dann Gefährdungsdelikt) bzw. Schädlichkeit eines Verhaltens auf der anderen Seite.[233] Im Rahmen eines verfassungsmäßigen *Tatstrafrechts* sei die Strafbarkeit immer an die konkrete Tat und nicht an die Persönlichkeit des Täters (dann *Täterstrafrecht*) gekoppelt.[234] Je weiter allerdings im Rahmen eines Vorbereitungsdelikts die Strafbarkeit vorverlagert wird, desto stärker rückt die Gefährlichkeit einer Person gegenüber der Gefährlichkeit einer Situation in den Vordergrund.[235]

Das Gefahrenabwehrrecht als Präventivmechanismus ist auf die Identifizierung, Einordnung und Bewertung von Gefahren angewiesen. Daher treffen die Ordnungsbehörden Prognosen über die Gefährlichkeit von Personen und Situation, um daraufhin unter Umständen auch unmittelbar freiheitseinschränkend wirkende Gegenmaßnahmen ergreifen zu können. Als Maxime gilt dabei generell die sog. Effektivität der Gefahrenabwehr. Jene Effektivität geht sogar dem Verursacherprinzip[236] vor, sodass regelmäßig derjenige von Maßnahmen betroffen sein wird, der die Gefahrenquelle am besten kontrollieren kann, auch wenn jener nicht der Urheber derselben ist. Dieser, auf Effektivität ausgerichteten, Primärebene

---

[232] Auch *Bäcker*, Kriminalpräventionsrecht, S. 319 ff., bedient sich dieser Systematisierung bei der Fragestellung, inwieweit kriminalpräventive Vorfeldtatbestände des materiellen Strafrechts das formelle Strafrecht in eine teil-präventive Ordnung umwandeln.

[233] Formal wurzelt die Trennung zwischen Strafrecht und Polizeirecht freilich auch in den Zuständigkeitsnormen des Grundgesetzes. Nach den Art. 70, 74 Abs. 1 GG ist das Strafrecht dem Kompetenzrahmen des Bundes und das Polizeirecht demjenigen der Länder zugeordnet.

[234] *Jescheck/Weigend*, Strafrecht AT, S. 54; *Sieber/Vogel*, Terrorismusfinanzierung, S. 138.

[235] *Hefendehl*, in ders. (Hrsg.), Grenzenlose Vorverlagerung, S. 89 (96); *Heinrich*, ZStW 121 (2009), 94 (117); *Paeffgen*, in: FS Amelung (2009), S. 81 (109 ff.).

[236] Siehe zum Begriff und den verschiedenen Ausprägungen im öffentlichen Recht *Lepsius*, Besitz und Sachherrschaft, S. 458 ff.

erst nachgelagert ist die sog. Gerechtigkeit der Lastenverteilung. Somit wird im Gefahrenabwehrrecht erst auf der Sekundärebene gegebenenfalls über die Billigkeit einer Inanspruchnahme entschieden. Zusammenfassend wird im Polizeirecht der Rechtsgüterschutz anhand von Wahrscheinlichkeitsberechnungen betrieben und mithilfe von Effektivitätsentscheidungen umgesetzt.

Auch wenn einzelne strafrechtliche Maßnahmen für sich genommen ganz ähnliche Wirkungen für den Betroffenen zeitigen oder sich subjektiv gleichermaßen freiheitseinschränkend anfühlen wie polizeirechtliche Maßnahmen,[237] sind beide Rechtsgebiete aus verfassungsrechtlicher Sicht dennoch unterschiedlich zu bewerten und offenbaren dadurch auch eine gestufte Eingriffsintensität. *Timm* etwa macht diese Unterscheidung im Rahmen ihrer Arbeit zur verfassungsrechtlichen Zulässigkeit der Einbeziehung der Gesinnung eines Menschen bei der Auswahl ordnungsrechtlicher und strafrechtlicher Maßnahmen an zwei Punkten fest. Erstens unterstütze das Strafrecht Verhaltensnormen und enthalte dadurch den Anspruch, absolut und abstrakt über die Einordnung einer gesellschaftlich missbilligten Handlung entscheiden zu können, während das Polizeirecht gewissermaßen wertneutralen und lediglich punktuellen Rechtsgüterschutz betreibe. Zweitens beinhalte das Strafrecht über die abstrakte Unwertentscheidung bezüglich einer Handlung hinaus auch die konkrete Tadelfunktion gegenüber einer menschlichen Verhaltensweise. Das Polizeirecht wiederum treffe auch im konkreten Einzelfall eine solche Entscheidung nicht, sondern versuche gewissermaßen wertfrei, drohende Rechtsgutsgefährdungen abzuwenden.[238] Dieser Analyse ist grundsätzlich zuzustimmen, wobei eine Verdeutlichung und eine Ergänzung vorzunehmen sind.

Erstens sind die genannten Aspekte durch den Begriff des strafrechtlichen Schuldprinzips zu präzisieren. Nicht nur ist dem Strafrecht gegenüber dem Polizeirecht der Anspruch der Entscheidungshoheit über Recht und Unrecht vorbehalten, vielmehr geht mit der Feststellung über den Unwert eines Verhaltens auch die Feststellung der Schuld des betroffenen Strafrechtsobjekts einher. Es wird also weder nur in abstrakter Form über die Abweichung eines Verhaltens von gesellschaftlichen Normen entschieden, noch in lediglich konkreter Art und Weise ein bestimmtes Verhalten als normbrechend beurteilt. Vielmehr sind die abstrakten und konkreten Elemente im Strafrecht kumulativ einzusetzen, sodass ein abstrakt missbilligtes Verhalten in seiner konkreten Form einer Person subjektiv vorwerfbar wird.

---

[237] *Frister*, Strafrecht AT, Kap. 1 Rn. 7 und *Heinrich*, ZStW 121 (2009), 94 (127), verdeutlichen dies am Beispiel des gezielten Todesschusses zur Gefahrenabwehr, der sogar stärker in die Rechtsgüter des Betroffenen eingreift, als es das repressive Strafrecht im Rahmen seiner verfassungsmäßigen Grenzen könnte.

[238] *Timm*, Gesinnung und Strafrecht, S. 124 f.

Beispiel: Die Herstellung von Hacking-Programmen wird eben nicht nur allgemein als rechtsbrechend eingeordnet, sondern gegebenenfalls auch konkret dem Hacker H als Urheber eines Programms zugeordnet. Über die Einordnung der Verwerflichkeit des Schreibens derartiger Programme hinaus wird H somit als Rechtsbrecher klassifiziert.

Das Polizeirecht verzichtet hingegen bei seinen Maßnahmen mindestens auf eines dieser Elemente, indem es, losgelöst von der gesellschaftlichen Ächtung eines Verhaltens oder der persönlichen Verantwortlichkeit für eine Rechtsgutsgefährdung, freiheitseinschränkende Eingriffe vornimmt.

Beispiel: Baseballschläger auf einer Demonstration werden gemeinhin als gefährlich wahrgenommen und daher oftmals verboten und ihren Besitzern abgenommen. Diese Maßnahmen ergehen grundsätzlich unabhängig davon, ob von dem Besitzer des Schlägers selbst tatsächlich eine Gefahr ausgeht. Die Einordnung der Gefährdungssituation wird mithin losgelöst von einem individuell vorwerfbaren Verhalten vorgenommen.

Letztlich kann dieser frühzeitige Eingriff nur deswegen verfassungsgemäß sein, weil er hiermit nicht auch über die Schuld des Betroffenen entscheidet und sich demgemäß auch eines Unwerturteils enthält. Während das Strafrecht also lediglich befugt ist, normativ zwischen Gut und Böse zu unterscheiden, kann das Polizeirecht schon im faktischen oder tatsächlichen Bereich Einfluss auf einen Geschehensablauf ausüben.[239]

Zweitens ist ergänzend die *Ultima-Ratio*-Funktion des Strafrechts als Unterscheidungskriterium gegenüber dem Polizeirecht anzuführen. Diese Maxime manifestiert sich darin, dass die strafrechtliche Reaktion stets als letztes Mittel gegenüber unrechtmäßigem Verhalten einzusetzen ist. Wenn also zivil- oder verwaltungsrechtliche Maßnahmen zur Konfliktlösung geeignet und ausreichend sind, ist eine rechtmäßige strafrechtliche Reaktion auf eine Verhaltensweise ausgeschlossen.[240] Erst wenn andere Rechtskreise tatsächlich durch äußerlich wahrnehmbares Verhalten beeinträchtigt werden, greift das Strafrecht ein.[241]

---

[239] Vgl. *Puschke*, in Hefendehl (Hrsg.), Grenzenlose Vorverlagerung, S. 9 (26), der in diesem Zusammenhang auch von einer problematischen Ablösung der strafrechtlichen Unrechtsbewertung durch die polizeirechtliche Effektivitätsbewertung spricht.

[240] *Baumann/Weber/Mitsch*, Strafrecht AT, § 3 Rn. 19; *Böse*, in: Hefendehl/von Hirsch/Wohlers (Hrsg.), Rechtsgutstheorie, S. 89 (94 f.); *Kaspar*, Präventionsstrafrecht, S. 243; *Zöller*, GA 2010, 607 (618); a. A. hingegen *Appel*, Verfassung und Strafe, S. 580; *Bäcker*, Kriminalpräventionsrecht, S. 365.

[241] Vgl. dazu die Folgerung zu *Jakobs* bei *Stegmann*, Organisierte Kriminalität: Feindstrafrechtliche Tendenzen 2004, S. 6, die hier den Begriff des Bürgerstrafrechts als Bezugs-

Doch was folgt aus diesen Abgrenzungskriterien? Und wie können sie bei der konkreten Frage nach der Einordnung einer Vorschrift behilflich sein? Beide Leitprinzipien des Strafrechts sind dazu in einer fraglichen Situation nebeneinander anzuwenden. Mithilfe des *Ultima-Ratio*-Grundsatzes ist festzustellen, ob der Regelungsbereich des Strafrechts überhaupt eröffnet ist, also ob zivilrechtliche und öffentlich-rechtliche Mittel nicht gleich geeignet zur Gewährleistung des Rechtsgüterschutzes sind. Das Schuldprinzip daneben verlangt dem Gesetzgeber die Begründung ab, weshalb ein konkretes Verhalten einer bestimmten Person in vorwerfbarer Weise als rechtsgutsbeeinträchtigend angelastet werden können soll. Während also der *Ultima-Ratio*-Grundsatz eine strafrechtliche Norm unter objektiven Gesichtspunkten beleuchtet, setzt das Schuldprinzip die gesellschaftliche Normgeltung mit dem Verhalten einer Person in Beziehung.

Die Vorbereitungsdelikte des Computerstrafrechts sind nach beiden Aspekten nicht dem Strafrecht zuzuordnen und daher nicht verfassungskonform. Zunächst ist äußerst fraglich, ob ordnungsrechtliche Eingriffsnormen zur Verhinderung der Rechtsgutschädigung nicht bereits ausreichend sind. Bei der Vorbereitung einer Computersabotage durch das Herstellen eines dazu geeigneten und bestimmten Computerprogramms etwa, wären viele Maßnahmen denkbar,[242] die sich eines Unwerturteils über das fragliche Verhalten enthalten. Um ganz grundsätzlich dem Schadenseintritt durch die Nutzung eines Hacking-Programms entgegenzuwirken, ist dessen Einziehung mit polizeirechtlichen Maßnahmen ausreichend. Eine strafrechtliche Qualifikation der Verhaltensweisen des „Täters“ ist hingegen nicht nötig.

Auch das Schuldprinzip wird über Gebühr strapaziert. Zwar ist grundsätzlich für jedes Verhalten eine rechtliche Norm formulierbar, die dem Wortsinn nach das Schuldprinzip beachtet, jedoch kann das Prinzip nur dann als erfüllt angesehen werden, wenn auch die Komponente des Rechtsgüterschutzes in die Bewertung mit eingeflossen ist. Das schützenswerte Rechtsgut ist vorliegend die Integrität eines Computers, Computersystems oder von Daten. Inwieweit das Verhalten eines „Täters“ in persönlich vorwerfbarer Weise dieses Rechtsgut zum Vollendungszeitpunkt geschädigt oder auch nur relevant gefährdet haben sollte, ist bei den computerstrafrechtlichen Vorfelddelikten nicht plausibel darzulegen. Das einzige Element der Norm, das tatsächlich auf eine potenzielle Gefährdung hindeutet, ist die Zweckbestimmung des Tatobjekts zur späteren Tatbegehung. Dass von einem solchen Tatobjekt eine potenzielle Gefährdung ausgeht, ist zwar kaum zu bestreiten, die Entscheidung über ein strafrechtliches

---

größe wählt und dadurch zum Ausdruck bringt, dass nur bei Beachtung des *Ultima-Ratio*-Grundsatzes von einem verfassungsgemäßen Strafrecht gesprochen werden kann.

[242] Siehe oben, Kap. 3 § 12 D.

Unwerturteil ist ohne Verstoß gegen das Schuldprinzip allerdings schlechterdings nicht zu erreichen.

Den gängigen Theorien folgend, wird das Strafrecht zwar auch als Vergewisserung einer Normgeltung eingesetzt, sodass der Rechtsgüterschutz durchaus in den Hintergrund treten kann, jedoch zumindest schlussendlich Teil der Strafbarkeitsrechtfertigung zu bleiben hat.[243] Im Sinne der General- und Spezialprävention soll das Strafrecht also auch vorbeugend wirken. Diese Wirkung hat sich allerdings auf die psychisch-präventive Komponente einer Strafnorm zu beschränken, sodass die pönalisierte Verhaltensweise in der Regel mit der zu verhindernden Tat deckungsgleich ist.[244] Vorliegend allerdings ist kaum wahrscheinlich, dass der Gesetzgeber tatsächlich die gesellschaftliche Ächtung des Herstellens eines bestimmten Computerprogramms herbeiführen will. Vielmehr ist er in präventiver Weise daran interessiert, dass diese Verhaltensweise im weiteren Verlauf nicht kausal für eine wirkliche Rechtsgutschädigung wird; etwa verursacht durch den Einsatz des Programms zur Computersabotage. Es wird also faktisch nicht versucht, einen vergangenen Konflikt zu verarbeiten oder die Geltung einer Verhaltensnorm für die Zukunft hervorzuheben, sondern vielmehr zukünftigen Gefahren entgegenzutreten.[245] Nicht die problematische Handlung wird mit Strafe bedroht, sondern eine angeblich diese problematische Handlung nach sich ziehende Verhaltensweise, was dazu führt, dass in diesen Fällen von einem Interventionsstrafrecht zu sprechen ist.[246]

Nach deutschem Verständnis handelt es sich bei den computerstrafrechtlichen Vorbereitungsdelikten mithin um Normen, die zwar ihrem Wortlaut nach strafrechtlich formuliert sind, inhaltlich jedoch dem Gefahrenabwehrrecht zuzuordnen sind. Sie sind weder *Ultima Ratio* noch konform mit dem Schuldprinzip, sondern reagieren auf durchaus existente Gefährdungssituationen mit Wahrscheinlichkeitsprognosen und unter Effektivitätsprämissen. Es geht nicht darum, den Unrechtsgehalt einer schädigenden Verhaltensweise durch Abschreckung zu unterstreichen und dadurch die Realisierung des Schadens oder der

---

[243] Es handelt sich dabei um die sog. positive Generalprävention, die eine „Normstabilisierung im Bewusstsein der Allgemeinheit“ anstrebt; vgl. im Einzelnen dazu *Roxin*, Strafrecht AT Bd. 1, § 3 Rn. 26 f.

[244] *Puschke*, in Hefendehl (Hrsg.), Grenzenlose Vorverlagerung, S. 9 (25). Als Beispiel führt er an, dass Totschlag und Mord schließlich die Tötung eines Menschen verhindern sollen und dass die Abschreckungswirkung eben nicht durch die Strafbarkeit der Planung einer Tötung erhöht wird.

[245] Vgl. *Gärditz*, Strafprozess und Prävention, S. 46, der dem Gesetzgeber zwar grundsätzlich die Befugnis zuspricht, ein „verpolizeirechtliches“ Strafrecht zu implementieren, aber dabei dennoch auf die Notwendigkeit abstellt, Vergangenes strafrechtlich zu bewerten.

[246] *Hefendehl*, in ders. (Hrsg.), Grenzenlose Vorverlagerung, S. 89 (95 f.); auch *Puschke*, in Hefendehl (Hrsg.), Grenzenlose Vorverlagerung, S. 9 (25 f.).

rechtlich relevanten Gefahr zu verhindern. Vielmehr soll bereits in einem frühen Stadium in den Geschehensablauf eingegriffen werden. Mithin handelt es sich hier um klassische polizeirechtliche Strukturmerkmale.[247]

b. Französisches Recht

Auch dem französischen Recht ist der sog. polizeiliche Dualismus (franz. *dichotomie policière*) inhärent, sodass die Polizei als *police administrative* und als *police judiciaire* gleichermaßen gefahrenabwehrrechtliche und straf(prozessual)rechtliche Aufgaben wahrnimmt. Obwohl der Grundsatz „Prävention vor Repression" auch dem französischen Sicherheitsrecht zugrunde gelegt wird, verläuft die Trennlinie zwischen präventiv-polizeirechtlichem und repressiv-strafrechtlichem Handeln im Vergleich zum deutschen Recht an anderer Stelle. Zwar sind die Begrifflichkeiten des französischen Rechts aus deutscher Perspektive wohlbekannt; als Einordnungskriterium wird nach herrschender Auffassung *le critère finaliste*, also der Zweck der Maßnahme herangezogen.[248] Jedoch werden dabei alle diejenigen Maßnahmen der *police judiciaire*, also den Strafverfolgungsorganen, zugeordnet, die bezüglich eines bestimmbaren Delikts erfolgen, auch wenn eigentlich die Verhinderung der Deliktsverwirklichung, mithin die Gefahrenabwehr, im Vordergrund steht.[249] Man kann also davon ausgehen, dass im französischen Recht strafrechtliche Kompetenzen bereits dann begründet werden, wenn ein Zusammenhang mit einer bestimmten oder bestimmbaren Straftat hergestellt werden kann.

Obwohl beide Rechtsordnungen die Trennung zwischen Polizei- und Strafrecht aus dem Grundrechtsschutz ableiten, ziehen sie dennoch unterschiedliche Schlüsse aus dieser Grundkonstellation. Während im deutschen Recht die mit einer strafrechtlichen Zuständigkeit einhergehenden Unannehmlichkeiten als besonders freiheitseinschränkend angesehen werden, wird bestmöglicher Grundrechtsschutz im französischen Recht dahin gehend verstanden, dass im Sinne eines *régime répressif* der Einzelne solange frei von staatlichen Eingriffen zu sein habe, wie er keine strafbare Handlung begeht.[250] Staatliche Eingriffe im Rahmen gefahrenabwehrrechtlicher Maßnahmen wären somit nach französischem Verständnis nicht zwangsläufig als milder gegenüber strafrechtlichen Maßnahmen einzuschätzen. Die genannte Trennlinie zwischen den Rechtsbereichen Gefahrenabwehr- und

---

[247] *Brodowski/Freiling*, Cyberkriminalität, S. 35, weisen insbesondere auch noch darauf hin, dass Vorverlagerungsstrafbarkeiten oftmals genutzt werden, um leicht nachweisbare Anknüpfungspunkte für weitergehende strafprozessuale Ermittlungsmaßnahmen bezüglich größerer Verbrechensstrukturen zu rechtfertigen.

[248] *Wittzack*, Vollzugspolizeien, S. 135 m. w. N.

[249] *Wittzack*, Vollzugspolizeien, S. 136.

[250] *Wittzack*, Vollzugspolizeien, S. 144 m. w. N.

Strafrecht ist damit derartig verschoben, dass gewisse nach deutschem Verständnis präventiv-polizeirechtliche Befugnisse in Frankreich durchaus der *police judiciaire*, also dem Bereich der Strafverfolgung zuzuordnen sind.

Im vorliegenden Fall der Vorbereitungshandlungen zu Computerdelikten stellen sich im französischen System mithin weniger Schwierigkeiten bei der strafrechtlichen Behandlung. Zwar ist erst die Erforschung derjeniger Delikte, welche die *police administrative* nicht verhindern konnte, den französischen Strafverfolgungsorganen zugeordnet,[251] jedoch wird im französischen Rechtskulturkreis eher ein übergriffiges Polizeirecht gefürchtet, während in Deutschland regelmäßig vor einer Zweckentfremdung präventiv-polizeirechtlicher Grundsätze für das Strafrecht gewarnt wird.[252]

c. *Spanisches Recht*

Prävention und Repression bezeichnen der Theorie nach ebenfalls im spanischen Sicherheitsrecht die maßgeblichen Unterscheidungskriterien zwischen der *policía administrativa* (Verwaltungspolizei) einerseits und der *policía judicial* (Gerichtspolizei) andererseits.[253] Die Einordnung in den Bereich der Prävention wird allerdings anders als im deutschen Recht nicht anhand des Zwecks der konkreten Maßnahme vorgenommen, sondern vielmehr mittels der Zuordnung in Tätigkeitsbereiche.[254] Ganz ähnlich wie in der französischen Praxis werden daher bei einem individualisierten Delikt sämtliche staatlichen Zuständigkeiten der *policía judicial*, also den Strafverfolgungsbehörden zugerechnet, auch wenn es sich sachlich eher um Gefahrenabwehr handelt.[255] Von einem tatsächlich individualisierten Delikt ist hierbei freilich kaum zu sprechen, sodass es vielmehr um ein sich später möglicherweise individualisierendes Delikt geht. Beispielhaft ist der polizeiliche Schusswaffeneinsatz zu nennen, der in Spanien ausnahmslos als Maßnahme der *policía judicial* eingeordnet wird,[256] während er nach deutschem Verständnis in den Polizeigesetzen der Länder geregelt wird. Die Differenzierung zwischen Gefahrenabwehrrecht und Strafrecht in Spanien findet mithin nach Sachbereichen statt, sodass ein sachlicher Zusammenhang

---

[251] *Wittzack*, Vollzugspolizeien, S. 133: Dabei handelt es sich laut *Wittzack* insbesondere auch um eine unmittelbare Folge der Französischen Revolution, indem die Gewaltenteilung durch die Aufspaltung in eine „Verwaltungs-“ und eine „Gerichtspolizei“ zum Ausdruck gebracht werden sollte.

[252] Auf das Strafprozessrecht bezogen: *Lisken*, NVwZ 1998, 22 (23) und *Waechter*, DÖV 1999, 138 (140).

[253] *Llera Suárez-Bárcena*, Poder Judicial 1993, 107 (108 f.).

[254] *Hinrichs*, Vollzugspolizei, S. 80.

[255] *Hinrichs*, Vollzugspolizei, S. 80.

[256] *Hinrichs*, Vollzugspolizei, S. 81, mit weiteren Beispielen.

mit einer (potenziellen) Straftat den Strafverfolgungsbehörden ganze „Befugnisbündel“ zuweist, auch wenn diese nach klassisch deutschem Verständnis dem Bereich der Prävention, also der Gefahrenabwehr zuzuordnen wären. In ähnlicher Form findet sich dieser „Bündel“-Ansatz etwa auch im EU-Recht, das zunächst einmal den gesamten Bereich der Computerkriminalität als strafrechtliche Materie einordnet.

Diese Praxis korrespondiert daher mit der Situation in Frankreich, wenngleich sie dort nicht gleichermaßen transparent gemacht wird. Dort wird zwar der Zweck einer Maßnahme als Abgrenzungskriterium genannt, allerdings faktisch weniger auf die konkrete Maßnahme, sondern vielmehr auf das dahinterstehende Ziel abgestellt. In tatsächlicher Hinsicht gleichen sich das spanische und das französische Sicherheitsrecht daher bei der Abgrenzung zwischen gefahrenabwehrrechtlichen und strafrechtlichen Kompetenzen, da jeweils bereits das Vorliegen eines individualisierten oder individualisierbaren Delikts als Anknüpfungspunkt für strafverfolgungsbehördliche Kompetenzen verstanden wird. Dieser Einordnung steht dabei nicht entgegen, dass es sich bei der Herstellung eines Computerprogramms eben nur um eine Vorbereitungshandlung handelt. Sämtliche Tätigkeiten, die dem später möglicherweise stattfindenden Delikt zuzuordnen sind, haben im spanischen Recht einen strafrechtlichen Bezug und gehören daher nicht mehr zur allgemeinen Gefahrenabwehr, sondern bereits zur spezielleren Strafverfolgung bezüglich eines noch nicht begangenen Delikts.

Auch nach spanischem Verständnis von Strafrecht dürfte Vorbereitungsdelikten im Computerstrafrecht damit wohl weniger Skepsis gegenübertreten.

d. Stellungnahme

Die Notwendigkeit einer Differenzierung zwischen Gefahrenabwehrrecht und Strafrecht ergibt sich aus mehreren Gründen, die sich darüber hinaus zwischen den jeweiligen nationalstaatlichen Modellen unterscheiden.

Im deutschen Recht kommt den Implikationen des föderalen Systems an dieser Stelle eine maßgebliche Rolle zu, da die Repressionslegislative als Strafrecht im Rahmen ausgeübter konkurrierender Gesetzgebungskompetenzen in den Zuständigkeitsbereich des Bundes fällt,[257] während präventive Maßnahmen als Polizeirecht den Bundesländern zugeordnet sind.[258] Abgesehen von dieser deutschen Besonderheit kommt der Abgrenzung allerdings auch in Frankreich da-

[257] Vgl. statt aller: *Degenhart,* in: Sachs (Hrsg.), GG, Art. 74 Rn. 10 ff.

[258] Diese ausschließliche Zuständigkeit der Länder folgt aus Art. 70 GG, da in den Art. 73 ff. GG das Polizei- und Ordnungsrecht nicht aufgeführt ist; vgl. statt aller: *Schenke*, Polizei- und Ordnungsrecht, § 2 Rn. 23.

durch eine Relevanz zu, dass entweder der verwaltungsrechtliche oder der ordentliche Rechtsweg eröffnet ist, wenn sich Betroffene gegen staatliche Maßnahmen zur Wehr setzen.[259] In Spanien hingegen ist eine derartige Rechtswegspaltung nicht vorgesehen, weshalb Betroffenen präventiv-polizeilicher oder repressiv-strafrechtlichen Maßnahmen gleichermaßen der Verwaltungsrechtsweg eröffnet ist.[260]

Die Einführung von Vorbereitungsdelikten in ein Strafrechtssystem erschwert die ohnehin oft schwierige Abgrenzung zwischen präventivem und repressivem Vorgehen der Polizei abermals. Durch dieselbe Handlung wird potenziell sowohl eine gefahrenabwehrrechtlich relevante Gefahr geschaffen, auf die mit polizeirechtlichen Präventionsmaßnahmen zu reagieren ist, als auch ein Straftatbestand verwirklicht, der die Polizei als Organ der Strafverfolgung zu repressiven Maßnahmen befugt.

Beispiel: Hacker H programmiert eine Computersoftware, um die IT-Steuerung eines Atomkraftwerks anzugreifen. Durch diese Handlung wird einerseits eine rechtlich relevante Gefahrenlage geschaffen, welche die Polizei- und Ordnungsbehörden zum Eingreifen ermächtigt, und andererseits womöglich der Straftatbestand der Vorbereitung einer Computersabotage nach §§ 303b Abs. 1 Nr. 3 i. V. m. 202c Abs. 1 StGB verwirklicht, was strafprozessuale Kompetenzen für die Strafverfolgungsbehörden nach sich zieht.

Zwar ist dieses Phänomen seinem Grundsatz nach unter dem Begriff der sog. doppelfunktionalen Maßnahmen bereits bekannt, sodass die daraus resultierenden Fragestellungen hinsichtlich des Rechtswegs hinreichend erforscht sind.[261] Insbesondere in „modernen" Kriminalitätsfeldern kommt es jedoch oftmals zu Überlagerungen, die über die Rechtswegfrage hinausgehen. Polizeirecht auf der einen und Strafprozessrecht auf der anderen Seite statuieren etwa unterschiedliche Eingriffsvoraussetzungen. Während die polizeiliche Generalklausel zur Ermächtigung präventiver Maßnahmen sehr große persönliche Einschränkungen zulässt, um Gefahren effektiv abwenden zu können, sind die strafprozessualen Eingriffsvoraussetzungen deutlich enger gefasst, da es sich regelmäßig um einen abgeschlossenen Sachverhalt handelt, aus dem sich keine akuten Gefahren mehr ergeben. Als weiterer Punkt ist die institutionelle Abschichtung der Verfahrensherrschaft zu nennen, die bei gefahrenabwehrrechtlichen Maßnahmen der Polizei und bei strafprozessualen Sachverhalten der Staatsanwaltschaft

---

[259] Siehe *Wittzack*, Vollzugspolizeien, S. 134.

[260] Siehe *Hinrichs*, Vollzugspolizei, S. 309 und 317.

[261] Eine zusammenfassende Übersicht bietet u. a. *Schmidbauer*, in: FS Steiner (2009), S. 734 (738 ff.).

zufällt.[262] Unabhängig vom Bezugspunkt der Abgrenzungsfrage besteht im deutschen Recht regelmäßig das Ziel einer klaren Entscheidung über das einschlägige Rechtsregime.

Im französischen Recht wird diese eher künstliche Aufspaltung zusammenhängender Lebenssachverhalte weniger strikt durchgehalten und argumentiert, dass verfassungsrechtlich nicht die Unterscheidung zwischen präventivem und repressivem Handeln von staatlichen Organen, sondern einzig und allein die strikte Einhaltung von Erforderlichkeits- und Verhältnismäßigkeitsgrundsätzen notwendig sei, um modernen rechtsstaatlichen Ansprüchen Rechnung zu tragen.[263]

Bei Übernahme des deutschen Vorbilds in das EU-Recht wäre mit den oben genannten Argumenten somit eine Nichtigkeit der Richtlinie bereits auf Ebene der Kompetenzbegründung anzunehmen, da trotz der strafrechtlichen Ausgestaltung materiell polizeirechtliche Harmonisierungen vorgenommen werden, für die eine Kompetenzgrundlage nicht zur Verfügung stünde. Folgt man hingegen dem Modell, für welches etwa das französische und spanische Recht exemplarisch stehen, indem strafrechtliche Zuständigkeiten bereits bei Bestehen eines zumindest individualisierbaren Delikts angenommen werden, können Vorbereitungshandlungen zu einem solchen durchaus in den strafrechtlichen Kompetenzbereich einbezogen werden und dann auch strafprozessuale Befugnisse auslösen. Als individualisiertes oder individualisierbares Delikt ist dabei das potenziell drohende Verletzungsdelikt (Bezugstat) einzuordnen, welchem das vorgelagerte Vorbereitungsdelikt als zugeordnet wird. Die Verhinderung einer drohenden Straftat ist damit bereits Teil des Strafrechts. Ein sich verstetigendes Interventionsstrafrecht wäre demgemäß kein bedrohliches Szenario wie im deutschen Recht, sondern vielmehr Ausdruck der aktuellen Kompetenzverteilung zwischen Polizei- und Strafrecht.

Während sich die spanische und zunehmend auch die französische Perspektive dem Verwaltungshandeln eher pragmatisch nähern und der Rechtstatsächlichkeit eine besondere Aufmerksamkeit schenken, ist der deutsche Ansatz bei der Differenzierung zwischen gefahrenabwehrrechtlichem und strafrechtlichem Handeln immer noch stark vom verwaltungs- und polizeirechtlichen Dualismus des 19. Jahrhunderts geprägt.[264] Dieses Grundprinzip wird eine besondere Ar-

---

[262] Besonders induktiv zu diesem Problemkomplex arbeitet *Bäcker*, Kriminalpräventionsrecht, S. 356 ff.

[263] *Decocq/Montreuil/Buisson*, Le droit de la police, S. 158 f. m. w. N. und unter Verweis auf die Entscheidung v. 12.1.1977, veröffentlicht im JO 15.1.1977, S. 344.

[264] *Mayer, O.*, Deutsches Verwaltungsrecht, S. 255 f., nahm bei der Entwicklung des deutschen Verwaltungsrechts gar Bezug auf das französische Verwaltungsrecht (*Mayer, O.*, Theorie des französischen Verwaltungsrechts, S. 153–221) und beschäftigte sich ausschließlich

gumentationskraft zugesprochen, auch wenn die tatsächliche Polizeirealität diese Nuancen abzubilden gar nicht mehr unbedingt imstande ist. Auch für den Bürger wirken präventive und repressive Maßnahmen, insbesondere wenn diese von derselben Behörde durchgeführt werden, oftmals gleich.

Obwohl gute Argumente für die Beibehaltung der strikten Trennung von Gefahrenabwehr- und Strafrecht vorliegen, worauf sogleich bei der Prüfung zum etwaigen Eingreifen von materiellen Begrenzungsklauseln einzugehen sein wird,[265] ist eine gesamteuropäische Verfassungstradition hinsichtlich einer restriktiven Trennung dieser beiden Rechtsbereiche entsprechend den deutschen Kriterien jedenfalls nicht auszumachen. Rechtsvergleichend lässt sich mithin konstatieren, dass bei der Zuordnung eines Normengefüges zum Strafrecht oder respektive zum Gefahrenabwehrrecht mit dem sachlichen Zusammenhang des finalen Zwecks einer Maßnahme ein durchaus anerkanntes Kriterium zur Verfügung steht. Verfassungstragende Gesichtspunkte, wie das *Ultima-Ratio*-Prinzip und der Schuldgrundsatz, die ausweislich des Manifests zur Europäischen Kriminalpolitik grundsätzlich europaweite Gültigkeit beanspruchen, können mithin nicht ausschließlich durch eine strikte Trennung der beiden Rechtsbereiche erfolgreich umgesetzt werden, sondern stattdessen etwa auch in den Erforderlichkeits- und Verhältnismäßigkeitsprüfungen von Einzelmaßnahmen ausreichend Beachtung finden.

Für die Einordnung der computerstrafrechtlichen Vorbereitungsdelikte bedeutet dieser Befund, dass rechtsvergleichende Aspekte darauf hindeuten, jene durchaus dem strafrechtlichen Bereich zuzählen zu können. Zumindest die spanische und die französische Rechtsordnung weisen keinen dem deutschen Recht vergleichbaren Konflikt an dieser Stelle auf. Die grundsätzliche Kompetenz der Europäischen Union zur Harmonisierung von Vorbereitungsdelikten in Kriminalitätsbereichen, die ihr gemäß Art. 83 Abs. 1 UAbs. 2 AEUV zugeordnet sind, besteht mithin.

Es stellt sich allerdings im Folgenden die Frage, ob durch die zwingend notwendige Beachtung materieller Grenzen einer Kompetenzbegründung, namentlich der nationalen Identitäten des Art. 4 Abs. 2 EUV, oder aber durch den sog. Notbremsemechanismus des Art. 83 Abs. 3 AEUV, auf der nachgelagerten Ebene der Europäischen Union das Ausübungsrecht bezüglich einer solchen Kompetenz abzusprechen ist bzw. für gewisse Mitgliedstaaten Abweichungsmöglichkeiten bestehen.

---

mit präventivem Polizeihandeln, da repressiv-polizeiliches Handeln für ihn nicht Bestandteil eines modernen Polizeirechts sein konnte.

[265] Kap. 3 § 12 D. II.

II. Materielle Grenzen und mitgliedstaatliche Abweichungsmöglichkeiten

Die Kompetenz aus Art. 83 Abs. 1 AEUV sowie ihre Ausübung unterliegen materiellen Grenzen, die sich nach dem EU-Primärrecht bestimmen lassen. Aus Art. 2 Abs. 1 EUV folgt ganz grundsätzlich zunächst, dass insbesondere die Achtung der Menschenwürde, der Freiheit, der Demokratie, der Gleichheit, der Rechtstaatlichkeit sowie die Wahrung der Menschenrechte fundamentale Werte der Union sind. Konkretisierend heranzuziehen sind die allgemeinen Rechtsgrundsätze und Grundfreiheiten, die Grundrechtecharta, die EMRK und das relevante Sekundärrecht.[266] In der strafrechtlichen Ausformung dieser Grundsätze sind vor allem der Grundsatz *nulla poena sine lege*[267], das Verhältnismäßigkeitsprinzip[268] und das Schuldprinzip[269] zu nennen. Als weitere strafrechtsspezifische Grenzen werden auch das *Ultima-Ratio*-Prinzip, die Rechtsgutslehre und das Bestimmtheitsgebot diskutiert.[270] Auch das bereits angesprochene strafrechtliche Schonungsgebot[271] ist in diesem Zusammenhang zu beachten.[272] Zwar hat die deutsche Rechtswissenschaft aus diesem Gedanken direkt ein konstitutionelles Prinzip gemacht und es überdies zu einem EU-rechtlichen Grundsatz erhoben, jedoch ist der Argumentationsstrang des besonders souveränitätsprägenden Strafrechts auch im wissenschaftlichen Diskurs anderer Mitgliedstaaten verankert.[273]

Dem hier gewählten Ansatz folgend, dass eine Einebnung von Unterschieden zwischen Gefahrenabwehrrecht und Strafrecht und damit eine übermäßige Kompetenzbegründung der EU droht, konzentrieren sich die Ausführungen zu den Grenzen des Strafrechts der EU auf die in diesem Zusammenhang besonders einschlägigen Aspekte: die nationale Identität der Mitgliedstaaten nach Art. 4 Abs. 2 S. 1 EUV[274] als materielle Grenze und das Instrument des Not-

---

[266] *Meyer*, in: von der Groeben/Schwarze/Hatje (Hrsg.), Art. 83 AEUV Rn. 27.

[267] *Gleß*, in Schomburg u. a. (Hrsg.), Rechtshilfe, Einf. Hauptteil III Rn. 49.

[268] EuGH, Rs. 94/71, Slg. 1972, 307, Rn 11 – *Schlüter & Maack*; Rs. 240/78 – Slg. 1979, 2137 – *Atalanta*; Rs. C-210/10, ECLI:EU:C:2012:64, Rn. 47 – *Urban*.

[269] EuGH, Rs. C-210/00, Slg. 2002, I-6453, Rn. 35 ff. – *Champignon Hofmeister*; *Meyer*, in: von der Groeben/Schwarze/Hatje (Hrsg.), Art. 83 AEUV Rn. 27; *Vogel/Eisele*, in: Grabitz/Hilf/Nettesheim (Hrsg.), 57. EL Aug. 2015, Art. 83 AEUV Rn. 35, 46.

[270] *Meyer*, in: von der Groeben/Schwarze/Hatje (Hrsg.), Art. 83 AEUV Rn. 31 f. m. w. N.

[271] Siehe oben, Kap. 2 § 7 D. III.

[272] Einen umfassenden Überblick zu materiellen Grenzen der Strafrechtsharmonisierung und der Wirkungsweise jener Grenzen bietet *Meyer*, in: von der Groeben/Schwarze/Hatje (Hrsg.), Art. 83 AEUV Rn. 27 ff. m. w. N.

[273] Vgl. etwa *Borgers*, in: Fijnaut/Ouwerkerk (Hrsg.), Police and Judicial Cooperation, S. 347 (354); *Luchtmann/Vervaele*, ULR 2014, 132 (133); *Topa*, SJLS 2012, 89 (97).

[274] Kap. 3 § 12 D. II. 1.

bremseverfahrens nach Art. 83 Abs. 3 AEUV[275] als prozessuales Mittel zur mitgliedstaatlichen Abweichungsmöglichkeit von EU-Sekundärrechtsakten. Dabei sind vor allem Inhalt und Reichweite der Vorschriften sowie deren rechtliche Einordnung im Mehrebenensystem zwischen EU und Mitgliedstaaten zu untersuchen und bei der Stellungnahme zur EU-Rechtmäßigkeit der Richtlinie 2013/40/EU heranzuziehen.[276]

1. Identitätsklausel des Art. 4 Abs. 2 S. 1 EUV

Die sog. Identitätsklausel verpflichtet die Europäische Union, die nationale Identität der Mitgliedstaaten zu achten, wie sie in ihren grundlegenden politischen und verfassungsmäßigen Strukturen zum Ausdruck kommt. Auch bei der „nationalen Identität" handelt es sich selbstverständlich um einen unionsrechtlichen Begriff,[277] der unionsrechtlich autonom und einheitlich auszulegen ist. Die EU-rechtliche Begriffsautonomie betrifft allerdings lediglich die Konturen, während den Mitgliedstaaten die Ausgestaltung des jeweiligen Begriffsinhalts im Rahmen eines gewissen Ermessensspielraumes zuzugestehen ist.[278] Art. 4 Abs. 2 EUV bietet somit zum ersten Mal einen gesetzlichen Rahmen, um mögliche Kollisionen zwischen Unionsrecht und dem Verfassungsrecht der Mitgliedstaaten auf normativer Ebene des Mehrebenensystems der Europäischen Union aufzulösen.[279]

Über eindeutige Bereiche (Staatlichkeit und Souveränität) hinaus ist nach dem Lissabon-Urteil des Bundesverfassungsgerichts auch „der demokratische Prozess gegen die schleichende inhaltliche Entleerung durch die Übertragung bestimmter, besonders identitätsstiftender Kompetenzen" durch Art. 4 Abs. 2

---

[275] Kap. 3 § 12 D. II. 2.

[276] Obwohl das Schuldprinzip und der *Ultima-Ratio*-Grundsatz oben unter Kap. 3 § 12 C. als problematische Faktoren bei den computerstrafrechtlichen Vorbereitungsdelikten ausgemacht worden sind und diese ebenfalls selbstständige unionsrrechtliche Grundsätze darstellen, wird auf eine explizite Kontrolle der Richtlinie anhand jener Maßstäbe im Rahmen dieser Arbeit verzichtet. Wie in Kap. 3 § 12 D. I. ausgeführt wird, sind diese Prinzipien zwar durchaus auch dem Unionsrecht zu entnehmen, haben aber bislang keine ausreichende Konkretisierung erfahren, um tatsächlich als materielle Schranken Wirkungen zeitigen zu können. Sie bleiben hinter den Anforderungen der nationalen Verfassungen derartig zurück, dass der Notbremsemechanismus als prozessuales oder politisches Mittel hier (zumindest noch) als zielführender angesehen wird.

[277] *von Bogdandy/Schill*, in: Grabitz/Hilf/Nettesheim (Hrsg.), 57. EL Aug. 2015, Art. 4 EUV Rn. 13; *Obwexer*, in: von der Groeben/Schwarze/Hatje (Hrsg.), Art. 4 EUV Rn. 27; *Streinz*, in ders. (Hrsg.), Art. 4 EUV Rn. 14.

[278] GA Maduro, Rs. C-213/07, Slg. 2008, I-2008, I-9999, Rn. 31 ff. – *Michaniki AE*; *Obwexer*, in: von der Groeben/Schwarze/Hatje (Hrsg.), Art. 4 EUV Rn. 27.

[279] *Wischmeyer*, AöR 140 (2015), 415 (442 f.).

S. 1 EUV geschützt. Namentlich fällt darunter u. a. auch das nationale Strafrecht.[280] An dieser Stelle wird eine Problematik der Mehrebenenkonstruktion innerhalb der Europäischen Union besonders deutlich. Das EU-Recht hat die nationalen Identitäten der Mitgliedstaaten zu achten. Da es sich dabei um eine EU-rechtliche Kategorie und Begrifflichkeit handelt, ist auch der EuGH dementsprechend ausschließlich auslegungs- und entscheidungsbefugt. Wenn aber der EuGH über den konkreten Inhalt einer mitgliedstaatlichen nationalen Identität entscheiden könnte, bestünde die Gefahr, dass dieser Schutz regelmäßig leerliefe. Somit ist eine Ausfüllung der Begrifflichkeit durch die jeweiligen mitgliedstaatlichen Verfassungsgerichte unabdingbar. Gleichwohl müssen auch diesen Grenzen gesetzt sein, da ansonsten die Politik der Europäischen Union unter Hinweis auf die nationale Identität durch die Mitgliedstaaten effektiv blockiert werden könnte. Sinnvollerweise können dem EuGH somit lediglich die Auslegungskompetenzen für die Konturen der Identitätsklausel und eine Art Verhältnismäßigkeitskontrolle hinsichtlich der verfassungsgerichtlichen Begriffsbestimmung auf mitgliedstaatlicher Ebene zufallen. Die konkrete Ausformung des Begriffs wird, nicht nur aus kompetenziellen Gründen, sondern vor allem auch wegen mangelnder Expertise des EuGH bezüglich der Identität eines Mitgliedstaats, den nationalen Verfassungsgerichten zufallen müssen.[281] Dass allerdings, im Sinne des Bundesverfassungsgerichts, das gesamte Strafrecht als Teil der nationalen Identität Deutschlands anzuerkennen wäre, darf wohl eher bezweifelt werden. Insbesondere die Tatsache, dass bereits strafrechtliche Kompetenzen auf die EU übertragen worden sind, spricht gegen die Absolutheit dieser These des Bundesverfassungsgerichts. Gewisse Besonderheiten eines jeweiligen mitgliedstaatlichen Strafrechtssystems werden hingegen als Teil der nationalen Identität einzuordnen sein. Für das deutsche Strafrecht ist in dieser Hinsicht etwa an die fehlende Strafbarkeit juristischer Personen oder die Strafbarkeit der Holocaustleugnung anzuknüpfen.

---

[280] BVerfGE 123, 267 (357).

[281] Dahin gehend zu verstehen sind vermutlich auch EuGH, Rs. C-287/98, Slg. 2000, I-6917 – *Linster*; Rs. C-373/00, Slg. 2003, I-1931 – *Truley*; Rs. C-103/01, Slg. 2003, I-5369 – *Kommission/Deutschland*; Rs. C-296/95) Slg. 1998, I-1605 – *EMU Tabac*; Rs. 327/82 Slg. 1984, 107 – *Ekoo*, die jeweils klarstellen, dass in denjenigen Fällen des EU-Rechts, in denen auf nationales Recht verwiesen wird, die Interpretationshoheit dem EuGH entzogen ist und stattdessen bei den mitgliedstaatlichen (Verfassungs-)Gerichten liegt; siehe auch *Borchardt*, in: Schulze/Zuleeg/Kadelbach (Hrsg.), Europarecht, § 15 Rn. 32; einen anderen, im Ergebnis aber wohl kaum abweichenden Ansatz wählt *Wischmeyer*, AöR 140 (2015), 415 (448), der unter Verweis auf GA Maduro, Rs. C-53/04 und C-180/04, Slg. 2006 I-07213, Rn. 39 f. – *Marrosu & Sardino* ein Zusammenspiel zwischen nationalstaatlichen Auslegungsergebnissen und europarechtlichen Wertungen des EuGH erkennt.

Rechtswirkungen entfaltet die Identitätsklausel in mehrfacher Hinsicht. Erstens ist es den Mitgliedstaaten unter Verweis auf den Schutz der nationalen Identitäten unter bestimmten Umständen gestattet, von unionsrechtlichen Verpflichtungen abzuweichen, indem die nationale Identität als legitimes Rechtfertigungsargument zur Beschränkung der Grundfreiheiten[282] vorgetragen wird.[283] Zweitens ist die nationale Identität der Mitgliedstaaten durch die Union beim Erlass von Sekundärrechtsakten zu achten,[284] sodass bei Verletzung derselben deren Nichtigkeit anzunehmen ist.[285] In diesem Fall ist wichtig, dass bereits der Eingriff in die nationale Identität eines Mitgliedstaats genügt, um die Nichtigkeit eines EU-Rechtsakts zu begründen.[286] Bislang wurde vor dem EuGH noch in keinem einzigen Fall die Nichtigkeit eines EU-Instruments aufgrund der Missachtung der nationalen Identität eines Mitgliedstaats angenommen.[287] Letztlich sind die Hürden auch derartig hoch angelegt, dass selbst bedeutende Verfassungswerte eines Mitgliedstaats seitens des EuGH nicht als identitätsstiftend angesehen werden.[288]

Das oben benannte *Ultima-Ratio*-Prinzip sowie der Schuldgrundsatz sind durchaus als identitätsstiftende Bestandteile des deutschen Strafrechts und damit auch des Verfassungsrechts zu bezeichnen.[289] Die Verpflichtung der Bun-

---

[282] Für den Binnenmarkt vgl. EuGH, Rs. C-202/11, EU:C:2013:239, Rn. 27 – *Las* und Rs. C-36/02, Slg. 2004, I-9609, Rn. 35 ff – *Omega*; für die Freizügigkeit vgl. EuGH, Rs. C-208/09, Slg. 2010, I-13693, Rn. 93 – *Sayn-Wittgenstein* und Rs. C-391/09, Slg. 2011, I-3787, Rn. 87 – *Runevic-Vardyn und Wardyn*.

[283] *von Bogdandy/Schill*, in: Grabitz/Hilf/Nettesheim (Hrsg.), 57. EL Aug. 2015, Art. 4 EUV Rn. 34; *Hatje* in Schwarze (Hrsg.), Art. 4 EUV Rn. 16; *Obwexer*, in: von der Groeben/Schwarze/Hatje (Hrsg.), Art. 4 EUV Rn. 35; ein Vertragsverletzungsverfahren der EU gegen den jeweiligen Mitgliedstaat wäre damit unbegründet und Haftungsansprüche ausgeschlossen.

[284] GA Wahl, Rs. C-58/13 und Rs. C-59/13, EU:C:2014:265, Rn. 101 – *Torresi*; vgl. auch *Hatje*, in Schwarze (Hrsg.), Art. 4 EUV Rn. 16; *Obwexer*, in: von der Groeben/Schwarze/Hatje (Hrsg.), Art. 4 EUV Rn. 36.

[285] EuGH, Rs. C-3/10, Slg. 2010, I-121, Tenor – *Affatato*; *Hatje*, in Schwarze (Hrsg.), Art. 4 EUVRn. 16; *Obwexer*, in: von der Groeben/Schwarze/Hatje (Hrsg.), Art. 4 EUV Rn. 35.

[286] Vgl. *von Bogdandy/Schill*, in: Grabitz/Hilf/Nettesheim (Hrsg.), 57. EL Aug. 2015, Art. 4 EUV Rn. 18; *Obwexer*, in: von der Groeben/Schwarze/Hatje (Hrsg.), Art. 4 EUV Rn. 36.

[287] Anmerkungen zu Verfahren, in denen sich der EuGH mit dem Begriff der nationalen Identität auseinandergesetzt hat, finden sich bei *von Bogdandy/Schill*, in: Grabitz/Hilf/Nettesheim (Hrsg.), 57. EL Aug. 2015, Art. 4 EUV Rn. 19 ff.

[288] Vgl. dazu insb. die Schlussanträge des GA Bot in der Rs. C-399/11, ECLI:EU:C:2012:600, Rn. 142 – *Melloni*.

[289] Bzgl. des Schuldprinzips insoweit zuletzt eindeutig BGHSt 59, 218 (239) und zuvor BVerfGE 123, 267 (413). Zusätzlich ist das Schuldprinzip bereits mehrfach auf die Menschenwürdegarantie des Art. 1 Abs. 1 GG zurückgeführt worden; BVerfGE 57, 250 (275); 80,

desrepublik Deutschland, einen Sekundärrechtsakt, hier die Richtlinie 2013/40/EU, in nationales Strafrecht umzusetzen und dabei Vorbereitungshandlungen zu implementieren, die gegen jene Prinzipien verstoßen,[290] könnte somit als Missachtung der nationalen Identität gewertet werden. Zusätzlich wäre darin unter Umständen ein Eingriff in die föderale Struktur Deutschlands zu erkennen, da gefahrenabwehrrechtliche Maßnahmen, die eigentlich dem Kompetenzbereich der Länder zugeordnet sind, durch den EU-rechtlichen Sekundärrechtsakt dem Strafrecht und damit dem Kompetenzbereich des Bundes zugeschlagen werden.[291] Konsequenterweise ginge mit diesem Ergebnis, in Anbetracht der bereits verworfenen Möglichkeit einer am deutschen Verfassungsrecht orientierten teleologischen Reduktion,[292] auch die Nichtigkeit der Richtlinie einher.

Dieses Ergebnis wird den Besonderheiten der Auslegung des EU-Rechts jedoch nicht ausreichend gerecht. Der Umstand, dass es sich bei der nationalen Identität um einen EU-rechtlichen Begriff handelt, der allerdings mitgliedstaatlich ausfüllungsbedürftig ist, stellt wahrscheinlich das relevanteste Beispiel für den bereits mehrfach angeführten Verfassungsgerichtsdialog im Mehrebenensystem der Europäischen Union dar.[293] Art. 4 Abs. 2 S. 1 EUV öffnet gewissermaßen das Unionsrecht gegenüber dem mitgliedstaatlichen Verfassungsrecht, das daraufhin aufgerufen ist, eine inhaltliche Konkretisierung vorzunehmen.[294] Der EuGH wiederum bestimmt letztlich die normative Reichweite des mitgliedstaatlichen Verfassungsrechts und nimmt dadurch die Auslegungsergebnisse nationaler Verfassungsgerichte in seine Entscheidungen *auf*, ohne diese jedoch zu *über*nehmen.[295] Anders ausgedrückt bedeutet dies, dass es sich bei der Verletzung nationaler Identitäten eher um *ein* Argument innerhalb des EU-rechtlichen Auslegungsvorgangs handelt, das im Gesamtzusammenhang der Verträge

---

367 (378); 90, 145 (173); hinsichtlich der europäischen Dimension dieser Strafrechtsprinzipien siehe die ausführliche Bearbeitung oben, Kap. 1 § 2 B. II. 1.

[290] Zum Verstoß siehe bereits oben, Kap. 3 § 12 D. I. 1. a.

[291] Die föderale Struktur ist nach ganz h. M. Bestandteil der nationalen Identität eines Mitgliedstaats. Siehe statt vieler: *Obwexer*, in: von der Groeben/Schwarze/Hatje (Hrsg.), Art. 4 EUV Rn. 32.

[292] Siehe oben, Kap. 3 § 12 D.

[293] Siehe oben, Kap. 2 § 7 C. I. 2. b. cc.

[294] *Mayer/Wendel*, in: Hatje/Müller-Graff (Hrsg.), EnzEuR Bd. 1, § 4 Rn. 257.

[295] Vgl. *Mayer/Wendel*, in: Hatje/Müller-Graff (Hrsg.), EnzEuR Bd. 1, § 4 Rn. 257 unter Verweis auf die Rechtsprechung des EuGH zur nationalen Identität als Rechtfertigungsgrund für Beeinträchtigungen der Grundfreiheiten: EuGH, Rs C-208/09, Slg. 2010, I-13693, Rn. 81–95 – *Sayn-Wittgenstein* und Rs C-391/09, Slg. 2011, I-3787, Rn. 83–94 – *Runevič-Vardyn*; siehe auch *Meyer*, in: von der Groeben/Schwarze/Hatje (Hrsg.), Art. 83 AEUV Rn. 33; *Pernice*, AöR 136 (2011), 185 (214 f.); *Reinbacher*, Strafrecht im Mehrebenensystem, S. 418.

zu verstehen ist.[296] Es vermag sich daher zwar durchaus gegen andere Prinzipien des Unionsrechts durchzusetzen, zwangsläufig tut es das allerdings nicht.[297]

Unabhängig vom grundsätzlichen Zusammenspiel der europäischen Verfassungsgerichte bei der Interpretation von Inhalt und Reichweite des Begriffs der nationalen Identitäten ist im vorliegenden Fall nicht von einer Nichtigkeit aufgrund einer Missachtung der nationalen Identität Deutschlands auszugehen. Die Identitätsklausel soll die Mitgliedstaaten unter anderem davor bewahren, durch die Umsetzung von EU-Rechtsakten ihre hergebrachten Verfassungswerte opfern zu müssen. In diesem speziellen Fall liegt die Gefahr eines solchen Zwangs jedoch nicht vor, sodass auch die Notwendigkeit einer umfassenden oder teilweisen Nichtigkeit der Richtlinie 2013/40/EU nicht besteht. Das liegt an der Existenz des Art. 83 Abs. 3 AEUV, dem sog. Notbremsemechanismus, der grundlegende mitgliedstaatliche Aspekte der Strafrechtsordnung zu schützen bestimmt ist.[298] Gewissermaßen handelt es sich beim Notbremsemechanismus also um eine spezielle Ausformung der Identitätsklausel,[299] sodass ein Rückgriff auf jene als „Generalklausel" für strafrechtliche EU-Rechtsakte gar nicht notwendig ist.

Man könnte also sagen, dass die Reichweite der nationalen Identitäten in Art. 4 Abs. 2 S. 1 EUV durch die Existenz des Notbremsemechanismus für strafrechtliche Sekundärrechtsakte eine Beschränkung erfährt. Durch die Schaffung eines strafrechtlichen *Opt-out* für einzelne Mitgliedstaaten (dazu sogleich) wird die Achtung der nationalen Identitäten im Strafrecht auf einen Kernbereich eingeengt. Die Rechtsposition der Mitgliedstaaten verschlechtert sich dadurch nicht. Zwar wird die Wirkung eines desintegrativ ausgestalteten Elements des EU-Rechts begrenzt, allerdings durch die Möglichkeit der Auslösung des Notbremseverfahrens mindestens aufgewogen. Das liegt vor allem daran, dass die Auslegungshoheit bezüglich der wirksamen Auslösung des Notbremsemechanismus sich bei den Mitgliedstaaten befindet (dazu sogleich), während die Elemente der Identitätsklausel als Begriffe des EU-Rechts grundsätzlich der EU-rechtlichen Auslegungsdomäne zugeordnet sind.

---

[296] *Pernice*, AöR 136 (2011), 185 (203); *Reinbacher*, Strafrecht im Mehrebenensystem, S. 418.

[297] Vgl. *Mayer*, in: von Bogdandy/Bast (Hrsg.), Europäisches Verfassungsrecht, 1559 (589 f.); *Mayer/Wendel*, in: Hatje/Müller-Graff (Hrsg.), EnzEuR Bd. 1, § 4 Rn. 257; *Pernice*, AöR 136 (2011), 185 (194 ff.); *Wischmeyer*, AöR 140 (2015), 415 (447); a. A. wohl noch *Doehring*, in: FS Everling Bd. 1 (1995), S. 263 (269 f.) und *Phelan*, Revolt or Revolution, S. 418.

[298] Statt aller: *Böse*, in: Schwarze (Hrsg.), Art. 83 AEUV Rn. 24.

[299] Ähnlich wohl auch *Meyer*, in: von der Groeben/Schwarze/Hatje (Hrsg.), Art. 83 AEUV Rn. 33.

Im Rahmen der Identitätskontrolle überprüft letztlich also der EuGH, ob das Schuldprinzip nach z. B. deutschem Standard tatsächlich von einem EU-Rechtsakt verletzt wird. Bei Auslösung des Notbremseverfahrens hingegen kann sich der jeweilige Mitgliedstaat selbstständig auf seine Verfassungstradition berufen. Die Überprüfung ist dabei (abgesehen von Missbrauchsfällen) der Auslegung durch den EuGH entzogen.

Plastisch ausgedrückt, müssen EU-primärrechtliche Prinzipien einen Mitgliedstaat nur solange schützen, wie dieser schutzbedürftig ist. Wenn jener aber durch die Option des Notbremseverfahrens den Schutz seiner Verfassungswerte selbstständig und gegebenenfalls sogar besser gewährleisten kann, ist der Rückgriff auf die Identitätsklausel des Art. 4 Abs. 2 S. 1 EUV einzuschränken. Dafür spricht insbesondere auch, dass die zuständigen Gewalten der Mitgliedstaaten in besonderer Weise mit den eigenen Verfassungstraditionen vertraut sind und damit in diesem beschränkten Bereich die Durchführung des Notbremseverfahrens vorzugswürdig erscheint.

Da Mitgliedstaaten, die ihre Strafrechtsordnung und somit die nationale Identität durch die Richtlinie 2013/40/EU berührt sehen, also Möglichkeiten zur Verfügung stehen, sich diesem EU-Rechtsakt zu verweigern,[300] ohne dessen Nichtigkeit herbeizuführen, ist nicht von einem Eingreifen der Identitätsklausel des Art. 4 Abs. 2 S. 1 EUV auszugehen.

2. *Auslösung des Notbremsemechanismus des Art. 83 Abs. 3 AEUV*

Wie bereits oben erwähnt,[301] ist durch den Vertrag von Lissabon mit Art. 83 Abs. 3 AEUV eine sog. verfahrensrechtliche Notbremse[302] eingeführt worden.[303] Danach kann ein Mitglied des Rats die Befassung durch den Europäi-

---

[300] Dazu sogleich, Kap. 3 § 12 D. II. 2.

[301] Siehe oben, Kap. 1 § 2 B. II.

[302] Weitere Notbremseverfahren im EU-Recht finden sich in Art. 48 Abs. 2; 82 Abs. 3; 86 Abs. 1 UAbs. 2 und 3; 87 Abs. 3 UAbs. 2 und 3 AEUV.

[303] Wortlaut des Art. 83 Abs. 3 AEUV: „Ist ein Mitglied des Rates der Auffassung, dass der Entwurf einer Richtlinie nach den Absätzen 1 oder 2 grundlegende Aspekte seiner Strafrechtsordnung berühren würde, so kann es beantragen, dass der Europäische Rat befasst wird. In diesem Fall wird das ordentliche Gesetzgebungsverfahren ausgesetzt. Nach einer Aussprache verweist der Europäische Rat im Falle eines Einvernehmens den Entwurf binnen vier Monaten nach Aussetzung des Verfahrens an den Rat zurück, wodurch die Aussetzung des ordentlichen Gesetzgebungsverfahrens beendet wird. Sofern kein Einvernehmen erzielt wird, mindestens neun Mitgliedstaaten aber eine Verstärkte Zusammenarbeit auf der Grundlage des betreffenden Entwurfs einer Richtlinie begründen möchten, teilen diese Mitgliedstaaten dies binnen derselben Frist dem Europäischen Parlament, dem Rat und der Kommission mit. In diesem Fall gilt die Ermächtigung zu einer Verstärkten Zusammenarbeit nach Artikel 20 Absatz 2 des Vertrags über die Europäische Union und Artikel 329 Absatz 1 dieses

schen Rat beantragen, wenn es der Ansicht ist, dass ein Richtlinienentwurf „grundlegende Aspekte seiner Strafrechtsordnung berühren würde“. Eine Ablehnung aus reinen Opportunitätsgesichtspunkten, etwa lediglich, um eine weitergehende europäische Integration generell zu verhindern oder zu verlangsamen, ist nicht ausreichend, sodass detailliert darzulegen ist, worauf die Unvereinbarkeit der Harmonisierungsmaßnahme mit nationalen Strafrechtsprinzipien zurückgeht.[304] Kommt es auch im Europäischen Rat nicht zu einem Einvernehmen, hat daraufhin eine Gruppe von mindestens neun Mitgliedstaaten vereinfachten Zugang[305] zur Verstärkten Zusammenarbeit nach Art. 326 ff. AEUV.[306]

Die Mitgliedstaaten erhalten auf diese Weise zwar nicht die Möglichkeit, eine strafrechtliche Richtlinie generell zu verhindern, jedoch ist der Notbremsemechanismus gewissermaßen als *Opt-out*[307] zu verstehen, sodass auch im Strafrecht ein sog. Europa der zwei Geschwindigkeiten denkbar ist.[308] Ausgelöst wurde der strafrechtliche Notbremsemechanismus bis dato freilich nicht.[309] Gerade dieses Element der Notbremse im Strafrecht der EU wird u. a. vom Bundesverfassungsgericht als Stärkung der mitgliedstaatlichen Rechte verstanden und ausdrücklich begrüßt, da etwa der deutsche Vertreter im Rat dazu verpflichtet ist, auf Weisung des Bundestages zu handeln,[310] was einfachgesetzlich in § 9 Abs. 1 IntVG[311] geregelt worden ist.

Exkurs: Problematisch erscheint diese gesetzliche Konstruktion zur Auslösung des Notbremsemechanismus durch den Vertreter im Rat (ggf. auf Weisung des Bundestags gem. § 9

Vertrags als erteilt, und die Bestimmungen über die Verstärkte Zusammenarbeit finden Anwendung.“

304 *Suhr*, in: Calliess/Ruffert (Hrsg.), Art. 83 AEUV Rn. 30.

305 Der grundsätzlich nach Art. 20 Abs. 2 EUV und Art. 329 Abs. 1 AEUV notwendige Ermächtigungsbeschluss gilt in diesem Fall als erteilt.

306 Die Verstärkte Zusammenarbeit nach Art. 20 EUV i. V. m. Art. 326 ff. AEUV ermöglicht die Abweichung von der einheitlichen Geltung des EU-Rechts. In bestimmten, durch die Voraussetzungen der Art. 326 ff AEUV festgelegten Fällen können daher mindestens neun EU-Mitgliedstaaten die Integration vorantreiben, ohne dass ein EU-weites Einvernehmen notwendig wäre. Siehe weiterführend und mit kritischen Anmerkungen *Thym*, EuR Beiheft 2/2013, 23 ff.

307 *Safferling*, Internationales Strafrecht, § 10 Rn. 63.

308 *Reinbacher*, Strafrecht im Mehrebenensystem, S. 482.

309 Das gilt i. Ü. für sämtliche Notbremsemechanismen des vergangenen und aktuellen Unionsrechts; siehe *Peers*, EL Rev 33 (2008), 507 (524).

310 BVerfGE 123, 267 (436); dem zustimmend auch *Ambos/Rackow*, ZIS 2009, 397 (403); *Suhr*, in: Calliess/Ruffert (Hrsg.), Art. 83 AEUV Rn. 35.

311 Gesetz über die Wahrnehmung der Integrationsverantwortung des Bundestags und des Bundesrates in Angelegenheiten der Europäischen Union (Integrationsverantwortungsgesetz) v. 22.9.2009; BGBl. I 2009, S. 3022; bzgl. der darin manifestierten Voraussetzungen vgl. *Böse*, ZIS 2010, 76 (89); *Suhr*, ZEuS 2009, 687 (710).

Abs. 1 IntVG bzw. des Bundesrats gem. § 9 Abs. 2 IntVG) aus der Perspektive des verfassungsrechtlich verankerten Gewaltenteilungsgrundsatzes. Die Entscheidung, ob eine auf Art. 83 Abs. 1 AEUV beruhende Richtlinie gegen grundlegende Aspekte der Strafrechtsordnung der Bundesrepublik Deutschlands verstößt, wirft zuallererst verfassungsrechtliche Fragen auf. Nach Art. 93 Abs. 1 GG kommt jedoch dem Bundesverfassungsgericht die Interpretationsverantwortung hinsichtlich des Grundgesetzes zu.

Art. 83 Abs. 3 AEUV selbst sieht lediglich ein Einschreiten des Ratsmitglieds vor. Die parlamentarische Rückbindung dieser Kompetenz geht letztlich auf das Lissabon-Urteil des Bundesverfassungsgericht zurück, das die Verfassungsmäßigkeit des Begleitgesetzes zum Vertrag von Lissabon von jener abhängig macht.[312]

Zwar würde die Auslösung des Notbremseverfahrens nach Art. 83 Abs. 3 S. 2 AEUV zunächst dazu führen, dass der Europäische Rat befasst wird, bevor ein tatsächliches „Opt-out" im Raum stünde, sodass grundsätzlich eine „vorbeugende" Auslösung der Notbremse denkbar wäre, um die betreffende Richtlinie einer umfassenden Kontrolle hinsichtlich ihrer Wirkungen auf die deutsche Strafrechtsordnung zu unterziehen. Da der strafrechtliche Notbremsemechanismus bislang allerdings noch nicht ausgelöst worden ist, wären die politischen Implikationen eines solchen Präzedenzfalls erheblich, sodass in der Praxis ein solcher Präventiv-Mechanismus kaum vorstellbar ist.

Da mithin sowohl die Exekutive (über das Ratsmitglied gem. Art. 83 Abs. 3 S. 1 AEUV) als auch die Legislative (durch den Bundestag/Bundesrat gemäß § 9 Abs. 1 und 2 IntVG) beteiligt sind, ist auch etwa ein Organstreitverfahren gem. Art. 93 Abs. 1 Nr. 1 GG wegen einer unterlassenen Auslösung der Notbremse nicht zu erwarten.

Schließlich kommt auch eine nachträgliche Kontrolle einer in Kraft getretenen EU-Richtlinie regelmäßig nicht in Betracht. Das ergibt sich, wie bereits gezeigt,[313] aus der Auslegungshoheit des EuGH zum Unionsrecht. Obwohl im Rahmen der sog. Identitätskontrolle Ausnahmen von diesem Grundsatz zu machen sind, betrifft das nur die gem. Art. 23 Abs. 1 S. 3 i. V. m. Art. 79 Abs. 3 GG für integrationsfest erklärten Grundsätze der Verfassung, namentlich Art. 1 GG und Art. 20 GG. Auch wenn weder Rechtsprechung noch Literatur bislang eine Ausdifferenzierung zu den grundlegenden Aspekten der deutschen Strafrechtsordnung vorgenommen haben, ist davon auszugehen, dass diese über jene integrationsfesten Grundsätze hinausgehen.

Damit ist nach der geltenden Gesetzeslage eine verfassungsgerichtliche Prüfung strafrechtlicher Richtlinien hinsichtlich ihrer Vereinbarkeit mit grundlegenden Aspekten der deutschen Strafrechtsordnung nicht vorgesehen. Lediglich für den deutlich engeren Bereich des unveräußerlichen Verfassungskerns hat sich das Bundesverfassungsgericht mittlerweile eine Kontrollbefugnis zugesprochen, sodass zumindest einige Fälle abgedeckt sind.[314] Obgleich die derzeitige Konstruktion mit Art. 83 Abs. 3 AEUV und die parlamentarische Rückkoppelung gem. § 9 Abs. 1 und 2 IntVG den Vorgaben des Bundesverfassungsgericht im Lissabon-Urteil entsprechen,[315] ist die fehlende Einbeziehung des Verfassungsgerichts als „Hüter der Verfassung" zu kritisieren. Grundsätzlich denkbar wäre daher, dass eine unionsrechtskonforme, gleichzeitig aber grundlegende Aspekte der deutschen Strafrechtsordnung

---

[312] BVerfGE 123, 267 (436); siehe dazu auch *Hahn*, EuZW 2009, 758 (759).

[313] Siehe oben, Kap. 2 § 7 C. I. 1.

[314] Zur Verankerung des Schuldprinzips in Art. 1 Abs. 1 GG und der damit einhergehende Auslegungskompetenz des BVerfG bei EU-Rechtsakten vgl. BVerfG NJW 2016, 1149 (1150 f.).

[315] Vgl. BVerfGE 123, 267 (436).

– freilich unterhalb der Schwelle zur Integrationsfestigkeit liegende – verletzende EU-Richtlinie von der deutschen Exekutive und Legislative unbeanstandet bliebe und dennoch eine Einwirkung durch das Bundesverfassungsgericht ausgeschlossen ist. Ein Leerlaufen des Notbremseverfahrens gem. Art. 83 Abs. 3 AEUV und auch des vom Bundesverfassungsgericht zur Absicherung gedachten § 9 Abs. 1 und 2 IntVG ist mithin insbesondere in solchen Fällen zu befürchten, in denen die Exekutiv- und Legislativorgane aus politischen Opportunitätsgesichtspunkten auf die Auslösung des Notbremsemechanismus verzichten. Die Legislativorgane der Bundesrepublik Deutschland wie auch die meisten anderen Parlamente in den EU-Mitgliedstaaten haben sich in der Vergangenheit regelmäßig äußerst zurückhaltend hinsichtlich ihrer Integrationskontrollbefugnisse verhalten,[316] sodass bei derzeitiger Konstruktion kaum eine Überprüfung der Vereinbarkeit von strafrechtlichen EU-Richtlinien mit grundlegenden Aspekten der Strafrechtsordnung zu erwarten ist.

Insbesondere wegen der relativen Seltenheit von strafrechtlichen EU-Richtlinien würde auch eine obligatorische verfassungsgerichtliche Überprüfung der darin enthaltenen Einflüsse auf die nationale Strafrechtsordnung nicht zu einer Arbeitsunfähigkeit der Europäischen Union führen. Zumindest bei offenkundigen Fällen oder wenn berechtigte Zweifel an der Vereinbarkeit einer EU-Richtlinie mit grundlegenden Aspekten der Strafrechtsordnung bestehen, wäre somit die Aufnahme einer zusätzlichen zwingenden verfassungsgerichtlichen Überprüfung im Rahmen des innerstaatlichen Verfahrens zum Notbremsemechanismus zu erwägen.

Zwar handelt es sich bei dem Merkmal der „grundlegenden Aspekte“ des Art. 83 Abs. 3 AEUV wiederum um eine primärrechtliche Begrifflichkeit, die grundsätzlich europarechtlich autonom zu interpretieren und zu konkretisieren ist.[317] Da allerdings bereits im Wortlaut von der „Auffassung“ des betroffenen Mitgliedstaats die Rede ist, wird nur dieser selbst beantworten können, ob derartige Aspekte seiner Strafrechtsordnung berührt sind.[318] Die Einschätzung, wann eine Richtlinie tatsächlich grundlegende Aspekte der Strafrechtsordnung berührt, ist somit den jeweiligen mitgliedstaatlichen Organen überlassen und durch den EuGH nicht überprüfbar,[319] sodass in diesem Instrument ein potenziell desintegrativ wirkender Baustein des EU-Rechts zu sehen ist.

---

[316] *Folz*, ZIS 2009, 427 (430), weist im Zusammenhang mit der Verabschiedung der Richtlinie 2008/99/EG über den strafrechtlichen Schutz der Umwelt darauf hin, dass diese zunächst wegen des noch nicht in Kraft getretenen Lissabon-Vertrags als Rahmenbeschluss verabschiedet werden sollte, letztlich aber wegen der fehlenden EU-Kompetenz in Art. 83 Abs. 1 UAbs. 2 AEUV über die Annexkompetenz des Art. 83 Abs. 2 AEUV ohne Beanstandung der mitgliedstaatlichen Parlamente zur Richtlinie umkonstruiert wurde.

[317] *Meyer*, in: von der Groeben/Schwarze/Hatje (Hrsg.), Art. 82 AEUV Rn. 54; *Satzger*, in: Streinz (Hrsg.), Art. 82 AEUV Rn. 67.

[318] *Peers*, EL Rev 33 (2008), 507 (527) spricht vom „benefit of the doubt“; i. E. wohl auch zustimmend *Meyer*, in: von der Groeben/Schwarze/Hatje (Hrsg.), Art. 82 AEUV Rn. 54; a. A. dagegen *Klip*, European Criminal Law, S. 478 f., der die Optionen für eine objektive Bestimmung der „grundlegenden Aspekte“ thematisiert.

[319] *Böse*, in Schwarze (Hrgs.), Art. 82 AEUV Rn. 39; *Dorra*, Legislativkompetenzen, S. 256; *Hecker*, in: Ambos (Hrsg.), Europäisches Strafrecht post-Lissabon, S. 13 (26); *Heger*,

Aufgrund dieser Interpretationskompetenz der Mitgliedstaaten sind deren jeweilige Rechtsetzungs- und -auslegungsorgane aufgerufen zu entscheiden, welche Aspekte der nationalen Strafrechtsordnung „notbremsefähig" sind. In Anbetracht des verhältnismäßig neuen Verfahrens gibt es bislang in Deutschland dazu noch keine gefestigte Praxis. Diesem Umstand ist auch geschuldet, dass in der strafrechtlichen Literatur reflexartig sämtliche Maximen des Strafrechts genannt und als konstituierend (v)erklärt werden. Verschiedenen Stimmen im Schrifttum zufolge gehören daher etwa das Legalitätsprinzip, der Parlamentsvorbehalt, das Verhältnismäßigkeitsprinzip, das Rückwirkungsverbot, das Schuldprinzip, das Rechtsgutsprinzip, das *Ultima-Ratio*-Prinzip, Strafzumessungskonzepte, Täterschaft und Teilnahme und weitere, teilweise sogar bereichsspezifische Prinzipien zu den grundlegenden Aspekten der Strafrechtsordnung.[320]

Vielen dieser vermeintlich grundlegenden Prinzipien gegenüber ist im Hinblick auf ihre Berücksichtigungsfähigkeit im Rahmen des Notbremseverfahrens durchaus Skepsis angebracht. Einerseits muss der betroffene Aspekt Ausdruck tief greifender und auch konstanter rechtskultureller Eigenheiten eines Mitgliedstaats[321] sowie in dessen Rechtssystem fest verankert sein.[322] Andererseits haben viele der genannten Prinzipien bereits eine EU-rechtliche Entsprechung gefunden oder sind bei nüchterner Betrachtung weniger konstituierend für das nationale Strafrecht als es die, insbesondere deutsche, Strafrechtswissenschaft glauben zu machen versucht.[323]

Die zuvor bereits genannten Prinzipien Rechtsgüterschutz, Schuldgrundsatz und *Ultima-Ratio*-Gedanke sind bei der vorliegenden Betrachtung von Vorbereitungsdelikten im Computerstrafrecht als mögliche Verstöße gegen grundlegende Aspekte der deutschen Strafrechtsordnung von besonderer Relevanz, sodass fraglich ist, ob jene tatsächlich im Rahmen von Art. 83 Abs. 3 AEUV vorgetragen werden könnten. *Meyer* hält das im Allgemeinen nicht für möglich, da es sich bei jenen größtenteils auch um anerkannte Grundsätze des EU-Rechts handele, die daher bereits auf der Stufe der Kompetenzbegründung justiziabel seien. Auf Ebene des Notbremsemechanismus seien damit allenfalls spezifische

---

ZIS 2009, 406 (414); *Reinbacher*, Strafrecht im Mehrebenensystem, S. 483; *Satzger*, in: Streinz (Hrsg.), Art. 82 AEUV Rn. 67.

[320] Vgl. *Hecker*, in: Sieber/Satzger/von Heintschel-Heinegg (Hrsg.), Europäisches Strafrecht, § 10 Rn. 46; *Meyer*, in: von der Groeben/Schwarze/Hatje (Hrsg.), Art. 83 AEUV Rn. 36; *Reinbacher*, Strafrecht im Mehrebenensystem, S. 483, jeweils m. w. N.

[321] *Dorra*, Legislativkompetenzen, S. 258; *Weigend*, ZStW 105 (1993), 774 (786 ff.).

[322] *Meyer*, in: von der Groeben/Schwarze/Hatje (Hrsg.), Art. 83 AEUV Rn. 36.

[323] Ausführlicher zu dieser Thematik *Meyer*, in: von der Groeben/Schwarze/Hatje (Hrsg.), Art. 83 AEUV Rn. 36 ff. m. w. N.

und dennoch gleichzeitig systemprägende nationale Lesarten einzelner Aspekte vorzutragen.[324]

Dem systematischen Argument, über Begriffe und Grundsätze des EU-Rechts auf Kompetenzbegründungsebene zu entscheiden, ist zuzustimmen.[325] Wenn nämlich nationale Verfassungsgerichte EU-rechtlich besetzte Begriffe und Grundsätze über den „Umweg" des Art. 83 Abs. 3 AEUV der Interpretationshoheit des EuGH entziehen könnten, bestünde die Gefahr, dass jene zumindest im Strafrecht faktisch ausgehöhlt würden. Allerdings kann diese Einschränkung nicht für derartige ausfüllungsbedürftige Begriffe des Strafrechts gelten, die auf EU-Ebene bislang keine dem nationalen Recht entsprechende Tiefe erlangt haben. Sollte nämlich wiederum bereits die EU-rechtliche Erwähnung oder gar implizite Anwesenheit von strafrechtlichen Grundprinzipien ohne eine theoretische und praktische Unterfütterung ausreichen, jene dem mitgliedstaatlichen Zugriff im Wege des Notbremseverfahrens zu entziehen, wäre diesem bewusst desintegrativ gehaltenen Instrument faktisch ebenfalls die Grundlage entzogen. Denn auf der Ebene der Kompetenzbegründung läge die Interpretationshoheit wiederum beim EuGH und die mitgliedstaatlichen Auslegungsansätze wären auf die Einbindung innerhalb eines gerichtlichen Dialogs beschränkt. Art. 83 Abs. 3 AEUV geht aber gerade über das Zusammenspiel im europäischen Verbund hinaus. Mindestens in denjenigen Fällen, in denen das EU-Recht keine eigenständige Dogmatik zu strafrechtlichen Grundsätzen entwickelt hat, ist demgemäß das Notbremseverfahren für die Mitgliedstaaten eröffnet und der Begriffsinhalt der Aspekte auf dieser Ebene nationalstaatlich zu bestimmen.

Vergleichbar wäre diese Konstellation etwa mit dem sog. Solange I-Beschluss des Bundesverfassungsgericht[326], da auch dort eine Kompetenz der nationalen Verfassungsgerichte für den Grundrechtsschutz angenommen worden ist, bis das Grundrechtsniveau auf EU-Ebene den jeweiligen mitgliedstaatlichen Level erreicht hat. Wie damals wäre auch hier bei der Differenzierung zwischen den Verfahrenswegen (Nichtigkeitsklage bei Begriffsinterpretationen des EU-Rechts und Notbremseverfahren bei grundlegenden Aspekten der nationalen Strafrechtsordnung) die Entscheidung hinsichtlich der Interpretationskompetenz davon abhängig, ob das EU-Recht sich selbstständig zu diesen Aspekten positioniert hat oder ob eine hinreichende EU-rechtliche Ausdifferenzierung

---

324 *Meyer*, in: von der Groeben/Schwarze/Hatje (Hrsg.), Art. 83 AEUV Rn. 37.

325 Auch *Reinbacher*, Strafrecht im Mehrebenensystem, S. 483 und *Vogel/Eisele*, in: Grabitz/Hilf/Nettesheim (Hrsg.), 57. EL Aug. 2015, Art. 83 AEUV Rn. 99, weisen auf die Vorrangigkeit der Kompetenzrüge im Wege der Nichtigkeitsklage nach Art. 263 AEUV in solchen Fällen hin.

326 BVerfGE 37, 271 ff.

bislang unterblieben ist. Freilich ist bei dieser Positionierung eine Deckungsgleichheit mit den nationalen Begriffsinhalten nicht notwendig, sodass durchaus eine abweichende Konstruktion gewählt werden kann. Lediglich das Niveau der begrifflichen Durchdringung auf EU-Ebene müsste derjenigen auf nationalstaatlicher Ebene entsprechen.

Bezüglich des *Ultima-Ratio*-Grundsatzes jedenfalls lässt sich derzeit keine EU-rechtliche Begriffstiefe feststellen. Unabhängig davon, ob man in diesem einen eigenständigen grundlegenden Aspekt der Strafrechtsordnung sieht oder das genannte Prinzip als Unterfall des Verhältnismäßigkeitsgrundsatzes einordnet,[327] findet es bislang im Strafrecht der Europäischen Union keine durchgängige Beachtung.[328] Teilweise wird gar gänzlich infrage gestellt, dass überhaupt eine Überprüfung und Begründung der Notwendigkeit einer Kriminalisierung bestimmter Verhaltensweisen stattfindet, sodass dieser Kernbereich eines verhältnismäßigen und am *Ultima-Ratio*-Grundsatz orientierten EU-Strafrechts unberücksichtigt bliebe.[329] Möglicherweise liegt das auch an der fehlenden Kenntnis der EU-Institutionen auf dem Gebiet des Strafrechts,[330] die unter anderem auf die binnenmarktorientierten Anfänge der Union zurückzuführen sein dürfte. Zwingend notwendig wäre dafür nicht einmal, dass bei strafrechtlichen EU-Sekundärrechtsakten der *Ultima-Ratio*-Grundsatz durchgängig im Sinne eines deutschen Verständnisses angewandt wird. Vielmehr würde es grundsätzlich genügen, wenn, einer strafrechtlichen *good governance* folgend, auf Aspekte der zurückhaltenden Kriminalisierung von menschlichen Verhaltensweisen eingegangen und gegebenenfalls begründet würde, weshalb im speziellen Fall vom *Ultima-Ratio*-Grundsatz abgewichen wird. Im Manifest zur Europäischen Kriminalpolitik wird indes nachgewiesen, dass insbesondere den Vorverlagerungstendenzen und Schritten zu einem Gesinnungsstrafrecht in vielen strafrechtlichen EU-Rechtsakten keine umfassende Begründung zur Abweichung vom Gebot des Strafrechts als *Ultima Ratio* bei der Steuerung unerwünschten Verhaltens gegenübergestellt ist.[331] Der *Ultima-Ratio*-Grundsatz als

---

[327] So u. a. *Meyer*, Strafrechtsgenese, S. 787 m. w. N.

[328] *Asp u. a.* (Manifest Kriminalpolitik), ZIS 2009, 697 (701).

[329] *Summers*, BJCLCJ 2015, 48 (54).

[330] So sieht es z. B. *Herlin-Karnell*, Criminal Law, S. 130 f.

[331] *Asp u. a.* (Manifest Kriminalpolitik), ZIS 2009, 697 (701 f.), mit Verweisen auf den Rahmenbeschluss zur Terrorismusbekämpfung (2008/919/JI, ABl. L 330 v. 9.12.2008, S. 21), den Rahmenbeschluss über Betrug und Fälschung im Zusammenhang mit unbaren Zahlungsmitteln (2001/413/JI, ABl. L 149 v. 2.6.2001, S. 1), den Rahmenbeschluss zur Bekämpfung der organisierten Kriminalität (2008/841/JI, ABl. L 300 v. 11.11.2008, S. 42) und den Rahmenbeschluss über Bestechung im privaten Sektor (2003/568/JI, ABl. L 192 v. 31.7.2003, S. 54).

Konkretisierung subsidiären Rechtsgüterschutzes ist mithin aktuell nicht als europäischer Rechtsgedanke existent.[332]

Auch hinsichtlich des Schuldgrundsatzes macht nicht nur die dem Manifest zur Europäischen Kriminalpolitik zugrunde liegende Untersuchung deutlich, dass eine Auseinandersetzung des EU-Gesetzgebers mit diesem grundlegenden Aspekt der (deutschen) Strafrechtsordnung nicht durchgängig erfolgt.[333] Auch an anderer Stelle wird darauf hingewiesen, dass Prinzipien wie Gesetzlichkeit, Verhältnismäßigkeit und Schuld, die ein verfassungsmäßiges Strafrecht überhaupt erst legitimieren, in der europäischen Kriminalpolitik bislang lediglich eine marginale Bedeutung erlangt hätten.[334]

Die Untersuchung führt gleichermaßen EU-Rechtsakte auf, deren Bestimmungen den Anforderungen des *Ultima-Ratio*-Grundsatzes respektive des Schuldprinzips Genüge tun und solche, die ohne deren Berücksichtigung zustande gekommen sind. Der Umstand, dass offensichtlich keine Regelmäßigkeit hinsichtlich des Einflusses universeller Verfassungsprinzipien auf die EU-Strafgesetzgebung besteht, unterstreicht deren bislang fehlende feste Implementierung im Rahmen einer Kriminalpolitik der Europäischen Union. Problematisch erweist sich daher auch nicht so sehr eine (vereinzelte) Missachtung der Prinzipien,[335] sondern vielmehr das bislang fehlende Grundverständnis für die Notwendigkeit ihrer flächendeckenden Beachtung oder zumindest Begründung einer Abweichung.

Sowohl das *Ultima-Ratio*-Prinzip als auch der Schuldgrundsatz lassen sich bereits jetzt aus dem EU-Primärrecht ableiten. Während der Verhältnismäßigkeitsgrundsatz[336] des Art. 5 Abs. 1 EUV das *Ultima-Ratio*-Prinzip mitumfasst,[337] fließt der Schuldgrundsatz aus der Unschuldsvermutung des Art. 48

---

[332] *Schaut*, Europäische Strafrechtsprinzipien, S. 246 ff. Jener weist darüber hinaus darauf hin, dass sich auch aus den einzelnen europäischen Rechtsordnungen kein eindeutiger dahin gehender Rechtsgrundsatz erkennen lässt; vgl. auch *ders.*, S. 265.

[333] *Asp u. a.* (Manifest Kriminalpolitik), ZIS 2009, 697 (702) führen insbesondere den Rahmenbeschluss zur Terrorismusbekämpfung (2002/475/JI, ABl. L 164 v. 22.6.2002, S. 3 [geändert durch Rahmenbeschluss 2008/919/JI, ABl. L 330 v. 9.12.2008, S. 21]) als Beispiel an.

[334] *Braum*, ZIS 2009, 418 (419).

[335] Das kommt bisweilen auch in mitgliedstaatlichen Rechtsordnungen vor, worauf *Prittwitz*, in: Ambos (Hrsg.), Europäisches Strafrecht post-Lissabon, S. 29 (33) treffend hinweist.

[336] *Melander*, EuCLR 2013, 45 ff. etwa erkennt sowohl in Subsidiaritätsprinzip als auch im Verhältnismäßigkeitsgrundsatz des EU-Rechts Ansatzpunkte für eine zukünftige Ausformung des *Ultima-Ratio*-Grundsatzes.

[337] Anders als der Wortlaut des Art. 5 Abs. 1 EUV zunächst vermuten lässt, bezieht sich der Verhältnismäßigkeitsgrundsatz nicht ausschließlich auf das Verhältnis zwischen Union und Mitgliedstaaten, sondern auch auf dasjenige zwischen öffentlicher Gewalt und Unionsbürger. In der Tat ist dieses Verhältnis sogar in der Vergangenheit das wichtigste Anwendungsfeld des Grundsatzes gewesen; vgl. *Kadelbach*, in: von der Groeben/Schwarze/Hatje

Abs. 1 GRC,[338] der Art. 6 Abs. 1 EUV folgend den EU-Verträgen gleichgestellt und damit Teil des Primärrechts ist.[339]

Damit sind beide zwar grundsätzlich im Normengerüst der Europäischen Union angelegt, sodass eine zukünftige begriffliche Ausformung und Schärfung, gegebenenfalls mit EU-rechtlichen Besonderheiten, möglich und im Hinblick auf die sich stetig erweiternden EU-Kompetenzen im Bereich des Strafrechts auch durchaus zu erwarten ist. Eine primärrechtliche Überprüfung mittels der Nichtigkeitsklage gegen spezielle Rechtsakte kann bis zu einer gleichwertigen begrifflichen Ausformung von Schuldgrundsatz und *Ultima-Ratio*-Prinzip im Vergleich zur deutschen Strafrechtsordnung aber noch nicht vorausgesetzt werden. Solange dieser Prozess aber lediglich in den Anfängen steckt,[340] muss den Mitgliedstaaten daher die Möglichkeit gegeben sein, im Wege des Notbremseverfahrens nach Art. 83 Abs. 3 AEUV grundlegende Aspekte der eigenen Strafrechtsordnung zu schützen.

(Hrsg.), Art. 5 EUV Rn. 49 unter Verweis auf die Rechtsprechung in EuGH, Rs. 41/79, Slg. 1980, 1979, Rn. 21 – *Testa/Bundesanstalt für Arbeit*; Rs. 265/87, Slg. 1989, 2237, Rn. 21 ff. – *Schräder/Hauptzollamt Gronau*; Rs. C-331/88, Slg. 1990, I-4023, Rn. 12 ff. – *The Queen/Fedesa*; Rs. C-133/93, Slg. 1994, I-4863, Rn. 41 – *Crispoltoni*.

[338] *Kaiafa-Gbandi*, EuCLR 2011, 7 (31); *Prittwitz*, in: Ambos (Hrsg.), Europäisches Strafrecht post-Lissabon, S. 29 (34).

[339] In seiner umfangreichen Untersuchung zum Schuldgrundsatz im EU-Recht kommt *Schaut*, Europäische Strafrechtsprinzipien, S. 219 ff., zwar zu dem Schluss, dass Art. 48 Abs. 1 GRC nicht heranzuziehen ist, der Schuldgrundsatz aber gleichwohl als ungeschriebenes EU-rechtliches Prinzip anzuerkennen ist. Dieses Ergebnis unterstützt die hier vertretene These, dass die relevanten EU-Institutionen den Schuldgrundsatz zwar anerkennen und ggf. würdigen, eine durchgehende und institutionalisierte Beachtung bei Rechtsetzung und Rechtsprechung allerdings bislang nicht stattfindet.

[340] Grundsätzlich ist auch einigen EU-Organen bewusst, dass das Strafrecht vorsichtig und prinzipiengeleitet eingesetzt werden muss, wie etwa die Erwähnung des Strafrechts als „letztes Mittel" zeigt; Rat der Europäischen Union, Vermerk v. 27.11.2009, 16542/2/09 REV 2 JAI 868 DROIPEN 160, S. 4. Die unmittelbare Reaktion der Europäischen Kommission auf den zuvor genannten Vermerk („Sie [die Kommission] ist jedoch der Ansicht, dass die Leitlinien und Musterbestimmungen in den Schlussfolgerungen des Rates verfrüht sind und zu einer verengten Auslegung von Artikel 83 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV) führen. Mit diesen Leitlinien und Musterbestimmungen legt der Rat einseitig einen Rahmen für die künftige Gesetzgebung fest, dem weder die Kommission noch das Europäische Parlament zugestimmt haben") illustriert dann auch das eher am Effektivitätsgrundsatz orientierte EU-Strafrechtsverständnis anderer EU-Institutionen; Erklärung der Europäischen Kommission zum Vermerk 16542/2/09 REV 2 JAI 868 DROIPEN 160, 16798/09 JAI 886 DROIPEN 163; abrufbar unter: http://register.consilium.europa.eu/doc/srv?l=DE&f=ST%2016798%202009%20INIT (Stand: 07.08.2017).

3. Zwischenergebnis

Die materielle Grenze der Identitätsklausel des Art. 4 Abs. 2 S. 1 EUV wird durch die Richtlinie 2013/40/EU nicht verletzt, sodass die Kompetenz der Europäischen Union zur Harmonisierung des Computerstrafrechts in diesem Rahmen gegeben ist.

Das Notbremseverfahren des Art. 83 Abs. 3 AEUV stellt aber gewissermaßen eine desintegrative Verfahrensgrenze des Unionsrechts dar. Anders als materielle Grenzen, vermag es nämlich die Richtlinie nicht unmittelbar zu ändern, sondern ermöglicht allenfalls eine Einflussnahme auf politischer Ebene durch die reine Androhung der Bremsziehung.[341] Die desintegrative Ausgestaltung des Verfahrens geht darauf zurück, dass von einem *Opt-out*-Mechanismus gesprochen werden kann,[342] indem Mitgliedstaaten in letzter Konsequenz ihre Teilnahme an einer Richtlinie verweigern und damit für die verbleibenden Staaten lediglich der vereinfachte Übergang zur Verstärkten Zusammenarbeit[343] bleibt.

Da sowohl das Schuldprinzip als auch und insbesondere der *Ultima-Ratio*-Grundsatz als grundlegende Aspekte des deutschen Strafrechts nicht hinreichend in der Richtlinie berücksichtigt worden sind, wäre es für den deutschen Vertreter im Rat oder für den Bundestag/Bundesrat möglich gewesen, das Notbremseverfahren in Gang zu setzen bzw. den Vertreter im Rat nach § 9 Abs. 1 und 2 IntVG dazu anzuweisen.[344] Wie gezeigt,[345] kommt eine nachträgliche Kontrolle der EU-Richtlinie durch das Bundesverfassungsgericht hingegen nur insoweit in Betracht, als die grundlegenden Aspekte der deutschen Strafrechtsordnung gleichzeitig als integrationsfeste Bestandteile des Grundgesetzes einzuordnen sind.

---

[341] *Meyer*, in: von der Groeben/Schwarze/Hatje (Hrsg.), Art. 83 AEUV Rn. 38, spricht in diesem Zusammenhang von „Verhandlungen im Schatten einer potentiellen Notbremse (*shadow of the emergency brake*)", weist diesem Vorgang aber keine herausragende Bedeutung für die Ziele von europakritischen Strafrechtlern zu; auch *Summers u. a.*, EU Criminal Law, S. 52, gehen davon aus, dass neben der tatsächlichen Ausübung die Androhung als Verhandlungsmittel für die Zukunft realistisch ist.

[342] *Safferling*, Internationales Strafrecht, § 10 Rn. 63.

[343] Siehe soeben, Kap. 3 § 12 D. II. 2.

[344] Eine Weisung der Legislative nach § 9 Abs. 1 und 2 IntVG ist dabei genauso hinreichend wie die selbstständige Entscheidung der Regierung; *Suhr*, in: Calliess/Ruffert (Hrsg.), Art. 82 AEUV Rn. 50 m. w. N.

[345] Siehe soeben, Kap. 3 § 12 D. II. 2.

III. Ergebnis zur (Teil-)Nichtigkeit von Richtlinie 2013/40/EU

Freilich erscheint die Auslösung des Notbremseverfahren hinsichtlich der Richtlinie über Angriffe auf Informationssysteme, die mit ihrer grundsätzlichen Zielrichtung zu unterstützen ist, in Anbetracht der relativ geringen Bedeutung der computerstrafrechtlichen Vorfeldtatbestände unverhältnismäßig. Es sollte sich allerdings die Frage stellen, ob Ermittlungs- und Beweiserleichterungen beim Schutz minder- bis mittelgewichtiger Rechtsgüter es wert sind, sich zunächst punktuell von einem tatbasierten Strafrecht zu verabschieden und stattdessen Elemente einer strafbaren Gesinnung einzuführen. Das *Ultima-Ratio*-Prinzip und der Schuldgrundsatz und in Teilen auch Aspekte des Rechtsgüterschutzes als Legitimation eines Strafrechtssystems sind nationalstaatlich in Deutschland so stark verankert, dass sie nicht für die schleichende Erweiterung des Strafrechts um sicherheitsrechtliche Elemente aufzugeben sind.

Der Notbremsemechanismus des Art. 83 Abs. 3 AEUV hat neben der rechtlichen Möglichkeit vor allem auch eine politische Dimension.[346] Er dient als Kompensation für die Aufgabe des Einstimmigkeitsprinzips bei strafrechtlichen EU-Rechtsakten. Ob durch dieses Erfordernis der expliziten Ablehnung eines Mitgliedstaats gegenüber einer strafrechtlichen EU-Richtlinie nicht möglicherweise ein besonderer Druck zur politischen Konsensfindung aufgebaut und dadurch zumindest faktisch die Wahrscheinlichkeit eines strafrechtlichen *Opt-outs* minimiert worden ist, kann bisher nur durch Vermutungen nahegelegt werden.[347] Der Umstand, dass es bislang noch nicht zum Einsatz des Notbremseverfahrens gekommen ist, bietet allerdings zumindest Indizien, in diese Richtung weiter zu beobachten und zu forschen. Da eine fundierte Forschung dazu auch in erheblichem Umfang auf politologische und sozialwissenschaftliche Methoden und Verfahren angewiesen ist, kann die Problematik im Rahmen dieser Arbeit allerdings lediglich angedeutet werden.

E. Zusammenfassung und Bewertung

Die aktuelle Richtlinie über Angriffe auf Informationssysteme harmonisiert EU-weit die sog. CIA-Delikte des Computerstrafrechts. Wie sich gezeigt hat, beschränkt sich die Europäische Union bei diesem Vorhaben auf den Kernbe-

---

[346] Siehe insb. *Peers*, EL Rev 33 (2008), 507 (528).

[347] So *Satzger*, in: Streinz (Hrsg.), Art. 83 AEUV Rn. 38; auch *Herlin-Karnell*, Criminal Law, S. 224 vermutet, dass es sich beim Notbremseverfahren um eine Art Scheininstrument handeln könnte, dessen tatsächliche Anwendung nicht beabsichtigt ist; diesen Erwägungen eher ablehnend gegenüber stehen *Vogel/Eisele*, in: Grabitz/Hilf/Nettesheim (Hrsg.), 57. EL Aug. 2015, Art. 83 AEUV Rn. 99.

reich des Computerstrafrechts und geht somit begrifflich nicht über den Kompetenztitel des Art. 83 Abs. 1 AEUV hinaus. Sämtliche aufgrund der Richtlinie zu harmonisierende bzw. harmonisierte Strafnormen lassen sich unter den hier vertretenen europarechtlichen Begriff der Computerkriminalität subsumieren. Mit dieser Erkenntnis geht gleichzeitig auch die grundsätzliche positive Einschätzung bezüglich Intention und Wirkungsweise der Richtlinie einher. Die Richtlinie beschränkt sich nicht nur auf den Kernbereich des Computerstrafrechts. Zusätzlich zielt sie ausschließlich auf Sachverhaltskonstellationen ab, deren transnationale Qualität oftmals naheliegt oder bei denen es lediglich vom Zufall abhängt, wenn Begehungs- und Erfolgsort innerhalb einer nationalen Jurisdiktion liegen. Daher unterstreicht sie umso deutlicher den Netzwerkaspekt eines engen Computerkriminalitätsbegriffs, wie er in dieser Arbeit vertreten wird.

Als weniger positiv ist allerdings, wie gezeigt, die sich verstetigende Tendenz zur Vorverlagerung der Strafbarkeit einzuordnen. Diese bringt für das deutsche Strafrecht nicht nur systematische Ungereimtheiten mit sich, sondern birgt die ganz grundsätzliche Gefahr, bereits die schädliche oder unerwünschte Gesinnung einer Person zur strafrechtlich relevanten Gefahr zu deklarieren, ohne dass sich der innere Entschluss zur Tat auch in einem nach außen gerichteten Tatverhalten bezüglich eines schützenswerten Rechtsguts manifestiert hätte. Insbesondere für Delikte zum Schutz von lediglich mittelrangigen Rechtsgütern erscheint eine Vorfeldkriminalisierung daher weder geboten noch notwendig. Die Richtlinie 2013/40/EU verdeutlicht damit die offensichtliche Tendenz des Strafrechts der EU, nicht nur bestehende nationale Regelungen anzugleichen und dabei auf verfestigte Strafrechtskonzepte zurückzugreifen. Sondern vielmehr ist ein extensiver Strafrechtsansatz erkennbar, der entweder gänzlich neue mitgliedstaatlich zu implementierende Straftaten schafft oder die Grenzen bestehender Strafbarkeiten ausdehnt.[348] Anstatt eines Schutzes des gesellschaftlichen, rechtlichen und ethischen Minimums bildet für die Europäische Union mithin vielfach die klassische Prävention die Basis des strafrechtlichen Schutzauftrags.[349]

Mit den oben genannten Gründen ist daher zwar noch von der EU-Rechtsmäßigkeit der Richtlinie 2013/40/EU auszugehen, gleichzeitig aber darauf hinzuweisen, dass für den deutschen Vertreter im Rat (ggf. auf Geheiß der nationalen Legislativorgane) durchaus die Möglichkeit zur Auslösung des Notbremsemechanismus nach Art. 83 Abs. 3 AEUV bestanden hätte. Die fehlende

---

[348] Vgl. auch *Borgers*, in: Fijnaut/Ouwerkerk (Hrsg.), Police and Judicial Cooperation, S. 347 (352 f.); *Summers u. a.*, EU Criminal Law, S. 279.

[349] Siehe auch *Mitsilegas*, EL Rev 34 (2009), 523 (536).

Einbeziehung des Bundesverfassungsgerichts bei der Überprüfung der Vereinbarkeit einer auf Art. 83 Abs. 1 AEUV basierenden EU-Richtlinie mit grundlegenden Aspekten der deutschen Strafrechtsordnung ist aus o. g. Gründen problematisch. Insbesondere im vorliegenden Fall wirkt sich dies auch aus. Zwar bleibt der Schuldgrundsatz nach aktueller Rechtsprechung des Bundesverfassungsgericht wegen seiner Zuordnung zur integrationsfesten Materie des Grundgesetzes bundesverfassungsgerichtlich überprüfbar,[350] sodass ein diesbezügliches Vorbringen in zukünftigen Verfahren vor dem Bundesverfassungsgericht hinsichtlich der Richtlinie 2013/40/EU denkbar ist. Das *Ultima-Ratio*-Prinzip des Strafrechts hingegen ist trotz seiner kaum zu bestreitenden Einordnung als grundlegender Aspekt der Strafrechtsordnung gleichwohl nicht den Art. 1 und 20 GG zuzuordnen,[351] sodass ein derartiges Vorbringen nach geltender unions- und nationalstaatlicher Rechtslage lediglich im Rahmen eines Notbremseverfahrens und nicht nachträglich möglich gewesen wäre.

---

[350] Siehe bereits oben, Kap. 1 § 2 B. II. 1. und BVerfG NJW 2016, 1149 (1150 f.).

[351] Zum *Ultima-Ratio*-Prinzip des deutschen Strafrechts vgl. insb. die obigen Ausführungen, Kap. 3 § 12 D. I. 1. a.

Kapitel 4

Perspektiven des EU-Computerstrafrechts

Nachdem sich die Teile 1 bis 3 dieser Arbeit allgemein mit den Mechanismen strafrechtlicher Harmonisierung und speziell mit dem europäischen Rechtsbegriff der Computerkriminalität des Art. 83 Abs. 1 UAbs. 2 AEUV als Harmonisierungsgrundlage sowie der Vereinbarkeit bisheriger computerstrafrechtlicher EU-Instrumente mit dem Primärrecht auseinandergesetzt haben, richtet der abschließende Teil 4 den Blick in die Zukunft. Wie gezeigt,[1] umfasst die Richtlinie über Angriffe auf Informationssysteme aus definitorischer Perspektive[2] nicht nur einen rechtmäßigen, sondern zudem auch äußerst relevanten Bereich beim Aufbau und zur Gewährleistung eines Raumes der Freiheit der Sicherheit und des Rechts innerhalb der Europäischen Union. Sowohl rechtswissenschaftliche als auch politische Debatten zur Computerkriminalität haben die Internationalität von Sachverhalten als eine Hauptschwierigkeit bei deren Bekämpfung ausgemacht.[3] Die Ubiquität von Computerdaten sowie die internationale Vernetzung einzelner Computer, ganzen Informationssystemen und letztlich sogar gesamten Infrastrukturen lösen die Auswirkungen von Computerstraftaten aus dem national beherrschbaren Raum heraus und stellen die EU und ihre Mitgliedstaaten durch die rasant wachsende Zahl transnationaler Bedrohungssituationen vor die Aufgabe, gemeinsam und grenzüberschreitend zu agieren, um diesem Aspekt einer europäischen Sicherheitsarchitektur[4] gerecht zu werden.[5] Die Ver-

---

[1] Siehe oben, Kap. 3 § 11 D.

[2] Hinsichtlich der Problematik zur Erfassung von Vorbereitungsdelikten siehe allerdings Kap. 3 § 12 C.

[3] Beispielhaft siehe KOM (2010) 245 endg./2, S. 20; *Sieber* u. a., Comprehensive Study on Cybercrime, 2013, S. XXIV ff.

[4] Die Grundfunktion eines Strafrechts als Instrument zur Gewährleistung von Sicherheit und Freiheit (dazu: *Roxin*, Strafrecht AT Bd. 1, § 2 C Rn. 7 ff.) findet sich mit entsprechenden Modifikationen auch im Europäischen Strafrecht allgemein und im Strafrecht der EU speziell wieder; dazu *Perron*, in: FS Küper (2007), 429 (436 ff.).

[5] Selbstverständlich ist letztlich nicht nur die Europäische Union, sondern vielmehr die gesamte internationale Gemeinschaft vor neue Herausforderungen der transnationalen Bekämpfung von Computerstraftaten gestellt. Allerdings ist die Europäische Union einerseits der unmittelbare Bezugspunkt dieser Arbeit und andererseits führt die Verzahnung innerhalb eines supranationalen Staatenverbundes zu besonders weitgehenden Erfordernissen der

ankerung einer expliziten Kompetenz zur Harmonisierung des materiellen Computerstrafrechts im AEUV und erste auf diese Kompetenz zurückgehende Richtlinien stellen im Vergleich zu anderen internationalen Initiativen und völkerrechtlichen Abkommen bereits eine deutlich intensivere internationale Integration des Rechts dar. Dass diese Maßnahmen auch für die Zukunft ausreichen werden, ist allerdings durchaus zweifelhaft.

Es darf wohl bereits als strafrechtliche Binsenweisheit aufgefasst werden, dass nicht das *law in the books,* sondern vielmehr das *law in action* für den „Erfolg" des materiellen und prozessualen Strafrechts entscheidend ist. Wenn es also um die Herausforderung einer transnationalen Verfolgung von Computerkriminalität geht, sind ein angeglichenes materielles Strafrecht und die europaweite Kooperation von Strafverfolgungsbehörden hilfreich, geboten und notwendig. Auf die tatsächliche staatsanwaltliche und gerichtliche Verfolgungspraxis können derartige angeglichene Regelungen jedoch zu wenig Einfluss ausüben. Die strafrechtliche Zuständigkeit der EU betrifft nämlich bislang lediglich die Gesetzgebung und nicht die Ausführung.[6]

Diese Tatsache ist aber aus zwei Gründen problematisch. Erstens ist maßgeblicher Hintergrund der Harmonisierung des materiellen Computerstrafrechts die Verhinderung sog. safe havens im EU-Raum. Zweitens basiert vor allem die Richtlinie gegen Angriffe auf Informationssysteme auf der Erkenntnis, dass die Informationsinfrastrukturen innerhalb der EU so stark vernetzt sind, dass Angriffe nahezu immer transnationale Auswirkungen haben. Als Grundlage anderer kritischer Infrastrukturen weisen die IT-Infrastrukturen in der EU gewissermaßen eine eigene Kritikalität auf.[7] Beide Gesichtspunkte deuten an, dass es über die harmonisierte Strafbarkeit sowie die koordinative Zusammenarbeit bei Aufdeckung und Verfolgung von Computerdelikten hinaus auch eines EU-weit gleichwertigen Niveaus des Strafverfolgungsinteresses bedarf.

In diesem Abschnitt wird daher der Frage nachgegangen, ob der im Bestehen befindlichen Europäischen Staatsanwaltschaft (EStA) die Zuständigkeit für die Verfolgung von Computerstraftaten übertragen werden sollte und könnte. Zunächst wird dazu herausgearbeitet, weshalb weitere Harmonisierungsschritte in diesem Kriminalitätsbereich überhaupt geboten sind. Darüber hinaus werden verschiedene denkbare Harmonisierungsmodelle für die Vertiefung der straf-

---

strafrechtlichen Zusammenarbeit. Ein hochaktuelles Beispiel zur Visualisierung der Notwendigkeit von internationalen Kooperationen bearbeitet *Goldberg*, CJEL 2015, 329 ff.

[6] *Schramm*, Internationales Strafrecht, § 4 Rn. 158, verdeutlicht es plastisch („Europol hat keine Pistolen."); siehe auch *Topa*, SJLS 2012, 89 (98).

[7] Dazu sogleich, Kap. 4 § 13 A.

rechtlichen EU-Integration vorgestellt[8] und schließlich wird begründet, warum einem sog. hybriden Modell an dieser Stelle der Vorzug einzuräumen ist.

§ 13 Informationssysteme als kritische EU-Infrastrukturen

Der Schutz kritischer Infrastrukturen ist eine der Kernaufgaben jedweder Staatlichkeit.[9] Neben Maßnahmen zur unmittelbaren Verhinderung von Sicherheitsvorfällen spielen auch strafrechtliche Sanktionen dabei eine wichtige Rolle, und zwar einerseits mit den Mitteln der General- und Spezialprävention und andererseits bei der effektiven Verfolgung und Bestrafung von kriminell verursachten Gefährdungen und Schäden.

Im Folgenden wird in aller gebotenen Kürze allgemein auf die Begrifflichkeit der kritischen Infrastrukturen eingegangen und festgestellt, dass Informationssysteme nicht nur kritische Infrastrukturen miteinander vernetzen, sondern auch selbstständig als kritische Infrastrukturen einzustufen sind. Schließlich wird begründet, dass die europäischen Informationsinfrastrukturen als ein genuines EU-Rechtsgut betrachtet werden können und damit ein Schutzbedürfnis unmittelbar durch die EU-Institutionen besteht.

A. IuK-Technologien als kritische Infrastrukturen

Kritische Infrastrukturen sind Organisationen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden.[10]

---

[8] Eine Übersicht zu verschiedenen Harmonisierungsmodellen bietet *Sieber*, Rechtliche Ordnung in einer globalen Welt, 2010, Initiative „MPG 2010+“ der Max-Planck-Gesellschaft; abrufbar unter: http://www.mpg.de/97975/HM01_Rechtliche_Ordnung-basetext.pdf (Stand: 07.08.2017).

[9] Vgl. u. a. *Bull*, Der Staat 47 (2008), 1 ff. m. w. N.; *Schmidt*, Der Staat 42 (2003), 225 ff.; *Sonntag*, IT-Sicherheit, S. 17 f.

[10] So die Definition des Bundesministeriums des Innern: Nationale Strategie zum Schutz Kritischer Infrastrukturen (KRITIS-Strategie);

abrufbar unter: http://www.bmi.bund.de/SharedDocs/Downloads/DE/Broschueren/2009/kritis.html (Stand: 07.08.2017). Etwas allgemeiner, aber im Grundsatz ähnlich formuliert *Schulze*, Bedingt abwehrbereit, 2006, S. 112: „Kritische Infrastrukturen sind staatliche und private Einrichtungen, die für das Gemeinwesen grundlegend notwendige (Dienst-) Leistungen anbieten. Stehen diese aufgrund von Störungen nicht oder nur eingeschränkt zur Verfügung, kann dies zu weit reichenden, nachhaltigen und lang andauernden Schäden führen. Diese Schäden können im Extremfall die Sicherheit eines Staates beeinträchtigen oder gefährden“. Außerdem findet sich in § 2 Abs. 10 S. 1 BSIG noch eine konkretere Legaldefiniti-

Regelmäßig werden einzelne Untergruppen und Sektoren gebildet, um verschiedene Industrien und Dienstleistungsbereiche dem Oberbegriff der kritischen Infrastruktur zuzuordnen. In Deutschland wird aktuell von 29 einzelnen Branchen, gruppiert in neun Sektoren, als kritische Infrastrukturen ausgegangen.[11] Unter den Begriff der Sektoren fallen beispielsweise Gesundheit, Wasser, Ernährung, Staat und Verwaltung, Energie sowie Medien und Kultur. Als Branchen werden hingegen die jeweiligen konkreten Infrastrukturbestandteile subsumiert, z. B. öffentliche Wasserversorgung, Labore, Börsen, Banken, Luftfahrt und Justizeinrichtungen.

Informationstechnik und Kommunikationstechnik bilden bei der Einordnung als kritische Infrastrukturen einen gemeinsamen Sektor und stellen gleichzeitig jeweils eine Branche dar. Die Kritikalität von IuK-Technologien ist demnach nicht von der Hand zu weisen. Anders als etwa den Infrastrukturbereichen Gesundheit, Wasser und Ernährung, kommt den IuK-Technologien allerdings noch eine weitere Dimension der Kritikalität zu, da sie nicht lediglich um ihrer selbst willen schützenswert sind,[12] sondern darüber hinaus auch Hilfseinrichtungen für die meisten anderen kritischen Infrastrukturen bezeichnen[13] und mithin gewissermaßen zusätzlich als Meta-Infrastrukturen anzusehen sind. Deutlich wird diese Einschätzung beispielsweise an der kritischen Infrastruktur des Finanz- und Versicherungswesens, die heutzutage ohne zuverlässig funktionierende IuK-Technologien nicht aufrechtzuerhalten ist.[14] Aktuelle wissenschaft-

on: „Kritische Infrastrukturen im Sinne dieses Gesetzes sind Einrichtungen, Anlagen oder Teile davon, die den Sektoren Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie Finanz- und Versicherungswesen angehören und von hoher Bedeutung für das Funktionieren des Gemeinwesens sind, weil durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden."

[11] Siehe https://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/Sicherheit/BevoelkerungKrisen/Sektoreneinteilung.pdf?__blob=publicationFile (Stand: 07.08.2017); In anderen Ländern kann diese Einordnung u. U. anders ausfallen, wie *Schulze*, Bedingt abwehrbereit, 2006, S. 114 f. rechtsvergleichend zwischen Deutschland und den USA nachweist.

[12] Dieser Schutz um ihrer selbst willen ergibt sich aus der Tatsache, dass in einer modernen partizipativen Gesellschaft die permanente Verfügbarkeit von Informations- und Kommunikationstechnologien als konstituierendes Element für ein mündiges Staatsvolk verstanden wird; so u. a. auch *König/Popescu-Zeletin/Schliesky*, Internet als kritische Infrastruktur, S. 24.

[13] *Greve*, DuD 2009, 756 (758), spricht folgerichtig bei den Informationstechnologien von einem Knotenpunkt beim Schutz kritischer Infrastrukturen.

[14] *Spannowsky*, in: ders./Runkel/Goppel (Hrsg.), Raumordnungsgesetz, § 2 Rn. 89.

liche Diskussionen zum Themenfeld der kritischen Infrastrukturen fokussieren sich demnach auch oftmals auf den Bereich der IT-Sicherheit.[15]

B. Vernetzung in der Europäischen Union

Diese aufgezeigte Doppelfunktion[16] als selbstständige kritische Infrastrukturen und Hilfseinrichtungen für andere kritische Infrastrukturen ist um eine zusätzlich, genauer ausgedrückt, daraus resultierende Besonderheit der IuK-Technologien zu ergänzen. Durch die Evolution der Nationalstaaten von abgegrenzten Einzelstaaten zu international eingebundenen und vernetzten Akteuren in einer globalisierten Welt sind kritische Infrastrukturen, die ausschließlich innerhalb eines nationalen Territoriums wirken, kaum noch vorstellbar. Insbesondere durch die (Rechts-)Integration innerhalb der EU sind die Wechselwirkungen zwischen verschiedenen Staaten derart umfangreich, dass Energie-, Transport-, Ernährung- und vor allem IuK-Infrastrukturen regelmäßig grenzüberschreitend genutzt werden. Sicherheitskonzepte für einzelne nationale Bestandteile dieser europäischen Infrastrukturen sind demnach zum Scheitern verurteilt,[17] da Beeinträchtigungen, Störungen und Angriffe beinahe zwangsläufig transnationale Auswirkungen haben.

Durch eine solch massive Vernetzung innerhalb der EU gewinnt die Kritikalität der IuK-Infrastruktur[18] eine neue, gar eine genuin europäische Dimension.

---

[15] Siehe u. a. verschiedene Beiträge in: *Holznagel* (Hrsg.), IT-Sicherheit; *Schulze*, Bedingt abwehrbereit; *Sonntag*, IT-Sicherheit.

[16] Von einer Doppelfunktion sprechen auch *König/Popescu-Zeletin/Schliesky*, Internet als kritische Infrastruktur, S. 10 f.

[17] Die Erwägungsgründe 2 („Informationssysteme sind für die politische, gesellschaftliche und wirtschaftliche Interaktion in der Union unverzichtbar. Die Gesellschaft ist in hohem und zunehmendem Maße von solchen Systemen abhängig. Das reibungslose Funktionieren und die Sicherheit dieser Systeme in der Union sind entscheidend […]“) und 3 („[…] es wächst die Besorgnis über mögliche Terroranschläge oder politisch motivierte Angriffe auf Informationssysteme, die Teil der kritischen Infrastruktur der Mitgliedstaaten und der Union sind. Hierdurch wird das Ziel einer sichereren Informationsgesellschaft und eines Raums der Freiheit, der Sicherheit und des Rechts gefährdet, so dass Gegenmaßnahmen auf Ebene der Union […] erforderlich sind.“) der oben in Kap. 3 § 11 ausführlich behandelten Richtlinie 2013/40/EU verdeutlichen das. *Greve*, DuD 2009, 756 (758), Fn. 30 nennt weitere Beispiele. Auch die KRITIS-Strategie, S. 16 macht auf den Umstand aufmerksam, dass der Schutz kritischer Infrastrukturen nicht auf Landesgrenzen beschränkt sein könne.

[18] Durchaus mit Recht verweisen *König/Popescu-Zeletin/Schliesky*, Internet als kritische Infrastruktur, S. 23 f., darauf, dass IT-Systeme und das Internet nicht per se als kritische Infrastrukturen einzuordnen sind, sondern stattdessen auf ihre jeweilige Bedeutung für andere kritische Infrastrukturen bzw. auf ihre eigenständige gesellschaftspolitische Kritikalität hin zu überprüfen sind. Diese Debatte soll hier jedoch nicht weiter vertieft werden, da für die vorliegende Untersuchung und Argumentation die Annahme hinreichend erscheint, dass

Die Funktionsfähigkeit von IuK-Infrastrukturen ist damit nicht mehr einfach nur ein Rechtsgut, dass in allen Staaten der EU schützenswert ist, weil ein einheitliches Niveau wünschenswert ist oder sich Störungen potenziell auf andere Mitgliedstaaten auswirken könnten.[19] Vielmehr kann quasi von einem „echten" EU-Rechtsgut ausgegangen werden.[20] Eine Prävention und Bekämpfung ist nämlich nicht nur effektiver auf transnationaler Ebene möglich, sodass die EU eine Art Hilfsfunktion für die Mitgliedstaaten ausfüllen würde, sondern vielmehr ist die EU zusätzlich selbstständig betroffen, wenn kritische IuK-Infrastrukturen gefährdet werden.

C. Vertiefte Integration für eine effektive Strafverfolgung und Bestrafung

Möglicherweise wäre bei einer Annahme eines solchen EU-Rechtsgutsstatus hinsichtlich der Funktionsfähigkeit der IuK-Infrastrukturen auch eine strafrechtliche Flankierung als Mittel der Prävention und Bekämpfung in Erwägung zu ziehen.

Eine diesbezügliche verstärkte Integration rechtfertigt sich durch potenzielle Bedrohungsszenarien bezüglich der IuK-Infrastrukturen. Beispielhaft sind dazu Angriffe auf die physische Struktur des Internets und anderer IT-Netzwerke, Angriffe auf die softwarebasierte Struktur von IT-Systemen sowie Angriffe auf die Kommunikationsübermittlung in IuK-Infrastrukturen etc. zu nennen.[21] Aufgrund der oben festgestellten Doppelfunktion der IuK-Infrastrukturen sind eine Verhinderung und Bekämpfung von Angriffen auf Informationssysteme im EU-Verbund nicht nur effektiver möglich, was regelmäßig als Begründungselement für bereits ausgeübte Harmonisierungskompetenzen herangezogen wird. Vielmehr ist die Funktionsfähigkeit der EU als solche durch Angriffe auf Informationssysteme, die entweder selbstständig kritische Infrastrukturen darstellen oder aber die Aufgabenerfüllung anderer kritischer Infrastrukturen überhaupt erst ermöglichen, bedroht.

---

maßgebliche Teile der IuK-Technologie, von denen das Internet und andere Netzwerke einen relevanten Teil ausmachen, eindeutig als kritisch sowohl für den nationalstaatlichen als auch für den unionalen Bereich zu klassifizieren sind.

[19] Vgl. u. a. *Greve*, DuD 2009, 756 (758).

[20] Richtlinie 2013/40/EU, Erwägungsgrund 3 spricht daher auch explizit von „Angriffe[n] auf Informationssysteme, die Teil der kritischen Infrastruktur […] der Union sind."

[21] Eine aktuelle und ausführliche Aufstellung und Analyse von relevanten Bedrohungsszenarien bieten *König/Popescu-Zeletin/Schliesky*, Internet als kritische Infrastruktur, S. 25 ff.

Damit geht die europäische Dimension beim strafrechtlichen Schutz von Informationssystemen sogar weiter als in anderen Bereichen, zu denen sog. Europa-Delikte[22] diskutiert werden. Jene Deliktskategorien beschränken sich regelmäßig entweder auf die Betroffenheit der EU als Kriminalitätsopfer oder die transnationalen Auswirkungen einer Kriminalitätserscheinung, um eine Zuständigkeit der EU herzuleiten. Die vorliegende Konstellation hingegen weist eine Kombination beider Begründungsansätze auf.

Die finanziellen Interessen der EU sind als Rechtsgut schützenswert, auch wenn es sich nicht um transnationale Sachverhalte handelt, da der Kernbestand der Rechtsgemeinschaft bedroht wird. Andere sog. Europa-Delikte, wie Drogen- und Menschenhandel, zeichnen sich hingegen dadurch aus, dass einerseits transnationale Verbrechen begangen werden und andererseits EU-weit anerkannte Rechtsgüter betroffen sind.

Die soeben dargestellte Relevanz der IuK-Infrastrukturen auch für nahezu sämtliche analoge kritische Infrastrukturen, die eigene Kritikalität und die bereits existente sowie stetig fortschreitende nicht nur europaweite Vernetzung legen somit die Notwendigkeit weitergehender Maßnahmen zur Harmonisierung des EU-Computerstrafrechts nahe. Im Folgenden sind demnach zukünftige Integrationsoptionen zur effektiveren Bekämpfung der Computerkriminalität im EU-Verbund aufzuzeigen sowie anhand anerkannter Harmonisierungsmodelle zu bewerten und auf ihre Umsetzbarkeit hin zu überprüfen.

§ 14 Harmonisierungsmodelle

In der geschichtlichen Entwicklung der Europäischen Union lassen sich schon seit langer Zeit strafrechtliche Elemente entdecken.[23] Erst im Rahmen aktuellerer Entwicklungen kristallisiert sich allerdings langsam die Strukturierung und Systematisierung eines Strafrechts der Europäischen Union heraus. Dabei lassen sich zwei argumentative Hauptstränge zur Begründung ausmachen: zum einen die Verfolgung der grenzüberschreitenden Kriminalität und zum anderen der strafrechtliche Schutz europäischer Rechtsgüter.[24]

---

[22] Zum Begriff der Europa-Delikte siehe *Tiedemann* (Hrsg.), Wirtschaftsstrafrecht in der Europäischen Union, Freiburger-Symposium; ferner zum Ursprung der Debatte *Cappel*, Untreuestrafrecht, S. 219 ff.

[23] *Jescheck*, ZStW 65 (1953), 496 ff. beschreibt eindrücklich die ersten Entwicklungen.

[24] Vgl. dazu *Sieber*, ZStW 121 (2009), 1 (3); *Summers u. a.*, EU Criminal Law, S. 276 ff.; *Zimmermann*, Strafgewaltkonflikte, S. 39.

Die dem hier vertretenen netzwerkspezifischen Computerkriminalitätsbegriff unterfallenden Computerdelikte haben mit beiden Grundpfeilern der EU-Strafrechtsharmonisierung maßgebliche Überschneidungspunkte. Dass bei kriminellen Aktivitäten zwischen Computer(netzwerke)n grenzüberschreitende Sachverhalte vorliegen, ist zwar nicht zwingend, jedoch sehr naheliegend und darüber hinaus auch aufgrund der nicht vorhersehbaren Datenflüsse oftmals zufällig und unbeherrschbar. Selbstverständlich ist die transnationale Qualität von computerstrafrechtlichen Sachverhaltskonstellationen nicht auf den rechtlichen Einflussbereich der Europäischen Union beschränkt. Nichtsdestotrotz sind einerseits die digitalen, wirtschaftlichen und gesellschaftlichen Abhängigkeiten zwischen den EU-Staaten oftmals enger als im globalen Bereich und andererseits wäre mit einem Hinweis auf die globale Dimension von politischen und gesellschaftlichen Themen beinahe jedweder Regulierungsansatz im Einflussbereich der Europäischen Union infrage zu stellen. Funktionierende transnationale Kooperationen und Rechtsharmonisierungen können hingegen vielmehr eine Modellwirkung für globale Regelungsmechanismen bieten.[25]

Die Betroffenheit von europäischen Rechtsgütern ist, wie gezeigt, zumindest bei Angriffen auf kritische IuK-Infrastrukturen anzunehmen. Von diesen beiden Prämissen ausgehend ist der Zuständigkeitsbereich eines Strafrechts der EU eröffnet. Daher ist im Folgenden klärungsbedürftig, welche Methoden der vertieften Strafrechtsharmonisierung denkbar, rechtlich gangbar, tatsächlich umsetzbar und empfehlenswert sind.

A. Ausbau der Zusammenarbeit

Eine Option zur Effektivierung des Strafrechts der Europäischen Union besteht in dem Ausbau der Zusammenarbeit bei Kriminalitätsbekämpfung und -verfolgung. In der Wissenschaft wird diese Form der Harmonisierung auch als sog. Kooperationsmodell bezeichnet.[26] Dabei entwickelt grundsätzlich jeder Mitgliedstaat sein eigenes formelles und materielles Strafrecht. Das gemeinschaftliche Vorgehen beschränkt sich einerseits auf die tatsächliche Ebene und andererseits auf rechtliche Instrumente der Zusammenarbeit, wie die klassische Rechts- und Amtshilfe. Dieser Systematik folgen regelmäßig die Ermittlungen im internationalen Raum außerhalb von besonderen Übereinkommen. Eine

[25] Im Bereich der Finanzmarktregulierung hat die Europäische Union bereits Rechtsinstrumente entwickelt, die auf globaler Ebene als Modellgesetze aufgegriffen worden sind, siehe dazu *Quaglia*, EUI SPS 2012/04; Gleiches gilt für das internationale Umweltrecht, siehe diesbezüglich *Inglis*, in: Dashwood (Hrsg.), EU external relations, S. 429 (452 f.); *Oberthür/Kelly*, The International Spectator 2008, 35 ff.

[26] Siehe exemplarisch *Sieber*, ZStW 121 (2009), 1 (17).

Souveränitätspreisgabe findet dabei letztlich gar nicht statt, da jeder Staat im Grundsatz in jedem einzelnen Fall über sein Tätigwerden zur Unterstützung des hilfeersuchenden Staats frei entscheidet.

In der Europäischen Union hat sich die klassische Rechts- und Amtshilfe mittlerweile zu einem System der Anerkennung justizieller Entscheidungen weiterentwickelt. Dabei wird in bestimmten kodifizierten Fällen auf die Entscheidungen eines anderen Mitgliedstaats vertraut. Als ein plastisches Beispiel für dieses Prinzip ist der Europäische Haftbefehl zu nennen.[27] Aus nationalstaatlicher Sicht stellt die Anerkennung fremder Gerichtsentscheidungen gegenüber einem verpflichtend vorgegebenen Strafrecht der EU einen weniger intensiven Eingriff in die staatliche Souveränität dar und wird somit weitgehend akzeptiert.[28]

Bei der Bekämpfung der Computerkriminalität weist die Zusammenarbeit innerhalb der EU insbesondere mit dem European Cybercrime Center als Abteilung von EUROPOL ein kooperativ angelegtes Element auf. Als Bestandteil von Europol sammelt es Daten, unterstützt die Mitgliedstaaten bei Ermittlungen und koordiniert gegebenenfalls auch transnationale Operationen zwischen den nationalen Strafverfolgungsbehörden. Außerdem ist auf das EU-Regime zum Datenaustausch nach dem sog. Verfügbarkeitsprinzip zu verweisen, bei dem ein direkter Zugriff auf die Informationsbestände bei mitgliedstaatlichen Strafverfolgungsbehörden gewährleistet werden soll.[29]

Obwohl die vertikalen (zwischen Mitgliedstaaten und EU) koordinativen Tätigkeiten des European Cybercrime Centers und insgesamt der horizontale (unmittelbar zwischen den jeweiligen Mitgliedstaaten) Ausbau von kooperativen Elemente im Strafrecht der EU beizubehalten und gegebenenfalls auszubauen sind, vermögen diese Ansätze den dringendsten Herausforderungen eines transnationalen Computerstrafrechts nicht hinreichend effektiv zu begegnen. Die Verhinderung von gravierenden Strafbarkeitsgefällen auf der einen und der

---

[27] Vgl. Rahmenbeschluss des Rates über den Europäischen Haftbefehl und die Übergabeverfahren zwischen den Mitgliedstaaten 2002/584/JI v. 13.6.2002, ABl. L 190 v. 18.7.2002, S. 1; eine ausführliche Übersicht mit aktuellen Entwicklungen zum Recht des Europäischen Haftbefehls findet sich bei *Klimek*, European Arrest Warrant.

[28] *Perron*, in: FS Küper (2007), S. 429 (435); Skepsis bleibt hinsichtlich dieser Art der gemäßigten Souveränitätsabgabe dennoch bestehen, wie das Urteil des BVerfG zum Ausführungsgesetz zum Europäischen Haftbefehl zeigt, in welchem ein besonderer Schutz deutscher Staatsbürger gefordert wird, siehe BVerfGE 113, 273 (299 f.).

[29] Implementiert durch den Rahmenbeschluss 2006/960/JI des Rates vom 18.12.2006 über die Vereinfachung des Austauschs von Informationen und Erkenntnissen zwischen den Strafverfolgungsbehörden der Mitgliedstaaten der Europäischen Union, ABl. L 386 v. 28.12.2006, S. 89; siehe dazu *Brodowski* in: Lange/Bötticher (Hrsg.), Cyber-Sicherheit, S. 249 (266) m. w. N.

Schutz gemeinsamer europäischer Rechtsgüter auf der anderen Seite sind durch die transnationale Zusammenarbeit von nationalen Behörden alleine nicht effektiv zu gewährleisten. Sog. safe havens[30] könnten bestehen bleiben und auch der Wille zur Strafverfolgung hinge weiterhin ausschließlich von den nationalstaatlichen Behörden ab.

Bei der Bekämpfung der Computerkriminalität bezeichnen kooperative Harmonisierungselemente somit gewissermaßen notwendige, nicht aber hinreichende Bausteine.

B. Ausbau der materiellen Integration

Einen Gegenentwurf zum Kooperationsmodell stellt die supranationale Harmonisierung des Strafrechts der EU dar.[31] Faktisch handelt es sich bei diesem Modell um die Ausdehnung eines Rechtsraumes im prozessualen und materiellen Bereich gleichermaßen. Entscheidungen würden nicht mehr nationalstaatlich gefällt und gegebenenfalls nach gemeinsamen Regelungen EU-weit anerkannt, wie etwa beim oben genannten Europäischen Haftbefehl. Stattdessen wird einheitliches Recht zentral zur Geltung gebracht. Für die EU ist etwa das Verwaltungssanktionsrecht bei Kartellverstößen beispielhaft aufzuführen.[32]

Bislang diskutierte Optionen zur vertieften Integration des Strafrechts der EU mit potenziellen Bezügen zur Bekämpfung der Computerkriminalität sind in den Initiativen für ein Europäisches Strafgesetzbuch[33] und für ein Strafgericht der EU[34] zu entdecken. Einen territorial noch darüber hinausgehenden Vorschlag macht *Schjølberg*, der die Schaffung eines internationalen Cybergerichtshofes anregt, um den Besonderheiten des Internets auf weltweiter Ebene gerecht werden zu können.[35]

I. Europäisches Strafgesetzbuch

Hinsichtlich eines gemeinsamen EU-Strafgesetzbuches verläuft der politische und wissenschaftliche Diskurs maßgeblich in Richtung der Etablierung eines

---

[30] *Zimmermann*, Strafgewaltkonflikte, S. 39, spricht von „Inseln der Straflosigkeit“.

[31] *Sieber*, ZStW 121 (2009), 1 (22 ff.).

[32] Vgl. Art. 23 Verordnung (EG) 1/2003, ABl. L 1 v. 4.1.2002, S. 16; vertiefende Hinweise zum Sanktionsrecht bei Kartellverstößen finden sich bei *Harding*, European Journal of Crime, Criminal Law and Criminal Justice, S. 275 ff.

[33] *Rosenau*, ZIS 2008, 9 ff.

[34] In diese Richtung argumentierend *Perron*, in: FS Küper (2007), S. 429 (440) m. w. N.

[35] *Schjølberg*, The Third Pillar for Cyberspace – An International Court or Tribunal for Cyberspace, 2014; abrufbar unter: http://www.cybercrimelaw.net/documents/140626_Draft_Treaty_text.pdf (Stand: 07.08.2017); siehe auch *Watney*, JITST 2012, 61 ff.

Allgemeinen Teils.[36] Dessen Ausarbeitung erscheint den Befürwortern geboten, um nationale Unterschiede bei strafrechtlichen Aspekten, wie Täterschaft und Teilnahme, Versuch, Unterlassen etc., aufzulösen und das Strafrecht diesbezüglich zumindest hinsichtlich derjenigen Bereiche zu vereinheitlichen, die bei transnationalen Sachverhalten regelmäßig relevant werden. Nur wenn diese Begrifflichkeiten des Allgemeinen Strafrechts unionsweit harmonisiert sind, können die Kompetenzen des Art. 83 Abs. 1 AEUV ihre volle Wirkung entfalten. Die bisherigen auf Art. 83 AEUV basierenden EU-Richtlinien behelfen sich in der Weise, dass die notwendigen AT-Definitionen jeweils in den Richtlinien-Text aufgenommen werden. Einerseits ist aber eine Konsistenz zwischen den verschiedensten Kriminalitätsbereichen so nur schwerlich zu gewährleisten und andererseits stellt sich die Frage, ob die Harmonisierungskompetenz des Art. 83 Abs. 1 UAbs. 2 AEUV überhaupt eine derartige Angleichung von Normen des Allgemeinen Teils umfasst.[37] Auch die Richtlinie über Angriffe auf Informationssysteme enthält solche AT-Definitionen[38] und Tatbestandsnormen, die mit Bestimmungen im Grenzbereich zwischen Besonderem und Allgemeinem Teil aufgeladen sind.[39]

Gegen eine umfangreiche Harmonisierung des Allgemeinen Teils des Strafrechts innerhalb der EU ist einzuwenden, dass diese zum einen immer noch nicht die gleichmäßige und effektive Verfolgung von bestimmten Kriminalitätserscheinungen wie der Computerkriminalität sicherstellen würde und zum anderen, dass im Primärrecht nach herrschender Auffassung bislang die notwendige Kompetenzgrundlage fehlt.[40] Auf absehbare Zeit ist demgemäß davon auszugehen, dass EU-Rechtsakte die jeweils notwendigen AT-Bestimmungen selbstständig aufnehmen, was regelmäßig als von der einschlägigen Kompetenzgrundlage abgedeckt angenommen wird. Dass allerdings AT-Normen unionsrechtskonform in die jeweiligen Sekundärrechtsakten integriert werden können, während gleichzeitig jedoch eine Harmonisierungskompetenz für eine umfassende Harmonisierung des Allgemeinen Teils nicht besteht, lässt sich freilich nur damit begründen, dass in diesem Falle auch Kriminalitätsbereiche betroffen wären, die (bislang noch) harmonisierungsfest sind. Ob ein derartiger

---

[36] Siehe u. a. *Long*, EIPA Scope, 2011, 49 (51).

[37] Siehe zu dieser Problematik *Kaiafa-Gbandi*, EuCLR 2015, 3 (11 ff.) m. w. N.

[38] Siehe oben, Kap. 3 § 11 B. VI.

[39] Bei Letzteren sei auf die oben geführte Diskussion zu den Vorbereitungsstrafbarkeiten im Computerstrafrecht verwiesen; Kap. 3 § 12.

[40] Es wird hingegen davon ausgegangen, dass die Union nach Art. 83 Abs. 1 AEUV kompetent zum Erlass von deliktsspezifischen AT-Vorgaben ist, wenn eine Angleichung insoweit für die wirksame Umsetzung der auf Art. 83 Abs. 1 AEUV beruhenden Richtlinien notwendig ist; siehe u. a. *Ambos*, Internationales Strafrecht, § 11 Rn. 11 Fn. 84; *Grünewald*, JZ 2011, 972 ff.; *Satzger*, Internationales und Europäisches Strafrecht, § 8 Rn. 27; *Stuckenberg*, in: Böse (Hrsg.), EnzEuR Bd. 9, § 10 Rn. 6.

Einfluss des EU-Strafrechts auf mitgliedstaatliche AT-Normen auf diese Weise tatsächlich unterbunden wird, muss unter Berücksichtigung auf die Diskussion zum Einfluss definitorisch weit gefasster Kriminalitätsbereiche auf verwandte Strafrechtsnormen allerdings bezweifelt werden.[41] Statt AT-Begriffe in jedem EU-Strafrechtsakt neu zu formulieren und gleichfalls eine Harmonisierung in Gang zu setzen, die, möglicherweise auch über den unmittelbaren Regelungsbereich hinaus, Auswirkungen in den mitgliedstaatlichen Strafrechtssystemen zeitig, wäre es ratsamer, die Anstrengungen für einen harmonisierten Allgemeinen Teil des Strafrecht zu unternehmen.

II. Strafgericht der Europäischen Union

Ebenfalls in den Bereich einer supranationalen Harmonisierung des Strafrechts fiele die Schaffung einer eigenständigen EU-Strafgerichtsbarkeit. Seitdem die Debatte über das Strafrecht der EU zur Mitte der 2000er-Jahre Fahrt aufgenommen hat, sind hinsichtlich der Gerichtsbarkeit verschiedene Modelle vorgeschlagen worden.

Befürworter gehen in der Regel davon aus, dass eine echte Strafrechtsintegration nur dann erreicht werden kann, wenn Europäische Staatsanwälte vor einem EU-Strafgericht auftreten und Anklagen vertreten.[42] Oftmals wird souveränitätsschonend darauf abgestellt, dass nach unterschiedlichen Kriterien lediglich bestimmte Straftaten vor einem solchen Gericht zu verhandeln sein sollten, wozu es dann klar voneinander abgegrenzter Zuständigkeiten bei der Verfolgung und Anklage bestimmter Straftaten zwischen den nationalen und den potenziell europäischen Strafgerichten bedürfe.[43] Zwar ist ein solcher Schritt mit dem derzeitigen Recht unvereinbar,[44] da der Europäischen Union lediglich die Kompetenzen zur Harmonisierung von Straftaten und Strafen in bestimmten Kriminalitätsbereichen übertragen worden sind,[45] während die Strafgewalt und -vollstreckung, mithin die Vollzugszuständigkeit, weiterhin im Zuständigkeits-

---

[41] Wegen des Anspruchs, eine stringente Gesetzessystematik zu gewährleisten, ist bereits jetzt denkbar, dass die auf EU-Rechtsakte zurückgehenden AT-Begriffe Einfluss auf weitere Definitonen des jeweiligen mietgliedstaatlichen Allgemeinen Teils haben; vgl. insoweit bereits oben, Kap. 2 § 7 B. I.

[42] Exemplarisch dazu *Perron*, in: FS Küper (2007), 429 (440).

[43] Siehe beispielsweise *Klip*, ZStW 117 (2005), 889 (900 ff.) in seinem Modellentwurf für ein Europäisches Strafjustizsystem; auch *Vogel*, in: Heß (Hrsg.), Wandel der Rechtsordnung, S. 45 (62 f.), macht detaillierte Vorschläge für ein europäisches Strafjustizsystem mit gegenüber den Nationalstaaten komplementär ausgestalteten Kompetenzen.

[44] *Langbauer*, Das Strafrecht vor den Unionsgerichten, S. 568; *Schramm*, JZ 2014, 749 (750); *Suominen*, MJ 2008, 217 (232).

[45] Vgl. statt aller: *Kugelmann*, in: Böse (Hrsg.), EnzEuR Bd. 9, § 17 Rn. 24.

bereich der Mitgliedstaaten verbleibt.[46] Tendenzen in Richtung einer strafrechtlichen Fachgerichtsbarkeit auf EU-Ebene sind demnach zunächst höchstens im Bereich der primärrechtlichen Kontrolle von EU-Rechtsakten zu erwarten.[47] Jedoch zeigen unter anderem Erfahrungen des US-amerikanischen Strafrechtssystems, dass parallel operierende Strafgewalten nicht undenkbar und sogar funktional sein können.[48]

Ein allgemeines Einheitsstrafrecht im Rechtsraum der EU wird bislang auf breiter Front abgelehnt[49] und erscheint derzeit auf wissenschaftlicher und politischer Ebene gleichermaßen weit entfernt. Überdies sind viele Bereiche des Strafrechts so stark national geprägt, dass eine trans- oder supranationale Instanz kaum vonnöten sein dürfte.[50] Ob dieser Befund auch für die Zukunft bestehen bleiben kann, soll an dieser Stelle dahinstehen. Die Identifikation von bestimmten Tatbeständen und Kriminalitätskategorien jedenfalls, die sich möglicherweise am Katalog des Art. 83 Abs. 1 UAbs. 2 AEUV orientieren könnten und die vor einem Strafgericht der EU anzuklagen wären, ist hingegen denkbar und weniger utopisch.[51]

Dass bei einem, wie auch immer ausgestalteten, Strafgericht der EU der Kriminalitätsbereich der Computerkriminalität als transnationales Kriminalitätsfeld schlechthin eine wesentliche Rolle spielen könnte, liegt nahe. Wie auch bezüglich eines Europäischen Strafgesetzbuches sieht das EU-Primärrecht jedoch derzeitig keine Kompetenz zur Errichtung eines Strafgerichts der EU vor.

III. Internationaler Cybergerichtshof

Einerseits enger umgrenzt, weil auf den Bereich der Cyberkriminalität beschränkt, und andererseits weiter gefasst, da als globales und den Vereinten Nationen untergeordnetes Gericht entworfen, zeigt sich der Vorschlag für einen internationalen Cybergerichtshof.[52] *Schjølberg* baut diesbezüglich auf den Ar-

---

[46] Vgl. *Böse*, in: ders. (Hrsg.), EnzEuR Bd. 9, § 27 Rn. 23; *Heger*, in: Giegerich (Hrsg.), Herausforderungen und Perspektiven der EU, S. 157 (161).

[47] *Langbauer*, Das Strafrecht vor den Unionsgerichten, S. 507 legt einen solchen Entwurf vor.

[48] Vgl. etwa *Hay*, US-amerikanisches Recht, Kap. 3 Rn. 106 ff. Ob eine Implementierung solcher paralleler Strafgewaltsysteme unter Aufrechterhaltung des Legalitätsprinzips möglich wäre, ist freilich zweifelhaft.

[49] Für die deutsche Strafrechtswissenschaft siehe insoweit *Hirsch*, ZStW 116 (2005), 835 (846) m. w. N.

[50] *Hirsch*, ZStW 116 (2005), 835 (846) m. w. N.; *Weigend*, ZStW 105 (1993), 774 (790 ff.).

[51] *Klip*, ZStW 117 (2005), 889 (900 ff.), zeigt beispielsweise den Weg zu einem solchen System auf.

[52] *Schjølberg*, The Third Pillar for Cyberspace – An International Court or Tribunal for Cyberspace, 10. Aufl., 2015.

beiten der relevantesten internationalen Akteure und Institutionen sowie auf mehreren Abkommen zur Cyberkriminalität auf. Als Hauptziel des Tribunals wird die Verfolgung und Bestrafung schwerwiegender Cyberattacken und Cyberdelikte mit globalem Interesse angegeben.[53] Insbesondere der strafrechtliche Schutz von kritischen IuK-Infrastrukturen wird in den Fokus dieses Entwurfs für ein völkerrechtliches Abkommen gerückt. Aber auch inhaltsbezogene und computerbezogene Delikte finden sich in dem Entwurf wieder, sodass, vom Bekämpfungsziel her verstanden, ein umfassender Ansatz bei der Bekämpfung der Cyberkriminalität vorgelegt wird, der als globales und judikativ-institutionelles Komplementär zu internationalen Instrumenten wie der Cybercrime Convention und ähnlichen Ansätzen der Vereinten Nationen anzusehen ist.

Die ins Stocken geratene Erweiterung der Anzahl von Unterzeichner- und Ratifikationsstaaten zur Cybercrime Convention[54] und die weitgehende Kapitulation der Vereinten Nationen bei der Entwicklung eines globalen Instruments zum formellen und materiellen Computerstrafrecht[55] zeigen allerdings, dass es Harmonisierungsmodelle mit derart weitreichenden Souveränitätspreisgaben schwer haben. Noch weniger als in einem bereits supranational ausgestalteten Rechtsraum wie der EU ist in naher Zukunft von der Errichtung eines (weiteren) internationalen Strafgerichtshof auszugehen. Folgerichtig verlagern internationale Organisationen, wie die Vereinten Nationen, der Europarat, die Weltbank, Interpol etc., ihre Anstrengungen bei der Bekämpfung von Computerkriminalität aktuell von einem umfassenden Harmonisierungsansatz auf die intensivere Verbreitung bestehender Instrumente und den Ausbau von technischen Fähigkeiten der Strafverfolgungsbehörden sowie auf die Erleichterung des Informationsaustauschs durch Errichtung von Kooperationseinrichtungen.[56]

Ein weiteres – hier allerdings aufgrund der damit verbundenen völkerrechtlichen Cyberwar-Dimension nicht zu vertiefendes – Hindernis bei der Errichtung eines solchen Cyberstrafgerichtshofes stellt die Tatsache dar, dass internationale Großmächte in den vergangenen Jahren Cyberattacken als wirksame und vermeintlich niedrigschwellige Mittel in Konfliktsituationen entdeckt haben. So erlitt Estland im Jahre 2007 einen großflächigen Cyberangriff durch DDoS-Attacken auf seine kritischen Infrastrukturen.[57] Infolge vorangegangener bilate-

[53] Wie auch *Watney*, JITST 2012, 61 (66), feststellt, sind nämlich gerade die umfangreichsten transnationalen IT-Attacken bislang nicht in zufriedenstellender Weise von Strafverfolgung betroffen.

[54] Siehe bereits oben, Kap. 3 § 11 E. I. 2.

[55] Siehe oben, Kap. 1 § 1 B. III.

[56] Siehe dazu weiterführend *Haase*, ZIS 2015, 422 ff.

[57] *Schulze*, Cyber-„War“, S. 27 f., führt den Erfolg der Attacken insb. auf den bereits damals sehr hohen Technisierungsgrad in Estland zurück („e-government“).

raler Differenzen wird gemeinhin vermutet, dass die Initiatoren aus Russland stammten.[58] Georgien wurde im Jahre 2008 im Rahmen des Russland/Georgien-Konflikts bereits knapp vor dem klassischen militärischen Angriff Russlands mit einer Cyberoffensive attackiert, sodass zum ersten Mal von einer Koordination zwischen Cyber- und Militäroperationen auszugehen ist.[59] Außerdem kam es im Jahre 2010 mit dem sog. Stuxnet-Wurm zu einem Cyberangriff auf die Atomanlagen Buschehr und Natan in Iran, sodass diese zeitweise außer Betrieb gesetzt wurden, obgleich die Urheberschaft des Angriffs bislang nicht eindeutig festgestellt werden konnte.[60]

Auch wenn die eingeschränkte Wahrscheinlichkeit der Unterzeichnung von relevanten Akteuren nicht per se gegen ein solches Vorhaben sprechen muss,[61] soll sich die hiesige Auseinandersetzung aufgrund des eher visionären Ansatzes in dieser überblickartigen Einführung erschöpfen.

IV. Zwischenergebnis

Anders als die oben genannten kooperativen Harmonisierungselemente, versprechen die hier untersuchten Vorschläge für eine Europäisches Strafgesetzbuch, ein allgemeines Strafgericht der EU und einen internationalen Cyberstrafgerichtshof durchaus Erfolgsaussichten bei der Bekämpfung der Computerkriminalität. Kaum ein Wissenschaftler, Praktiker oder Politiker würde wohl die Vorteile bei der europäischen oder globalen Zentralisierung oder zumindest vollumfänglichen Harmonisierung der Strafgewalt für einen solchen transnationalen Deliktsbereich leugnen. Insbesondere in der Strafrechtswissenschaft werden allerdings auch die Nachteile einer Erweiterung der Strafrechtskompetenzen der Europäischen Union thematisiert, wobei vor allem auf den Verlust der nationalen Souveränität, die Verwässerung gewachsener Strafrechtssysteme und Verfassungsprinzipien sowie die Nutzung des Strafrechts als reinen Durchsetzungsmechanismus für zivil- und ordnungsrechtliche Zwecke abgestellt wird.[62]

---

[58] Vgl. *Lesk*, IEEE Security and Privacy 2007, 76 ff.

[59] *Schulze*, Cyber-„War“, S. 28 f.; *Tikk u. a.*, Cyber Attacks Against Georgia, S. 4 f.

[60] Siehe *Falliere/Murchu/Chien*, Stuxnet Dossier, 2011, für vertiefende Hinweise zum Angriff und den Theorien zur Urheberschaft. Letztlich gehen diese aber nach überwiegender Auffassung auf Israel und die USA zurück; vgl. *Schulze*, Cyber-„War“, S. 16 m. w. N.

[61] Der Internationale Strafgerichtshof wird nicht von allen Groß- und Regionalmächten unterstützt und sowohl bei der Auswahl wie auch beim Erfolg der durchgeführten Verfahren regelmäßig kritisiert und leistet dennoch große Dienste im Bereich der internationalen Strafgerichtsbarkeit.

[62] Siehe statt vieler: *Schmölzer*, ZStW 123 (2011), 709 (719 f.); *Schünemann*, ZIS 2009, 393 ff.; *Weigend*, ZStW (116) 2004, 275 (282 ff.).

Bislang hat jedoch freilich keiner der vorgestellten Ansätze tatsächlich das Potenzial zur Umsetzung in geltendes Recht, da zurzeit weder in der EU noch auf globaler Ebene ein politischer Wille zur weitreichenden Souveränitätspreisgabe oder auch nur zur Einigung auf Grundprinzipien im Computerstrafrecht besteht.

C. Kompetenzausweitung einer Europäischen Staatsanwaltschaft

Für das Untersuchungsobjekt dieser Arbeit, den EU-Verbund als Akteur bei der Kriminalitätsbekämpfung, bietet jedoch möglichweise das sog. gemischte oder hybride Harmonisierungsmodell eine Option zur vorsichtigen Vertiefung der europäischen Integration im Computerstrafrecht. Eine Grundannahme bildet dabei das Ziel der weitgehenden Beibehaltung von nationaler Souveränität zur materiellen Strafrechtsetzung in Kombination mit einer zentralen Behörde zur Strafverfolgung in begrenzten Zuständigkeitsbereichen. Die Ermächtigung der in Gründung befindlichen Europäischen Staatsanwaltschaft zur Ermittlung und Anklageerhebung bei Computerdelikten könnte der grenzüberschreitenden Dimension von Sachverhalten gerecht werden und gleichzeitig einer möglichweise „schädlichen" Einebnung nationaler Besonderheiten vorbeugen. Im folgenden Abschnitt wird daher zunächst in der gebotenen Kürze die Europäische Staatsanwaltschaft hinsichtlich ihrer Aufgabenbereiche,[63] des institutionellen Aufbaus,[64] ihrer Befugnisse[65] und des aktuellen Stands im Errichtungsprozess vorgestellt,[66] bevor anschließend der Kriminalitätsbereich der Computerkriminalität bezüglich seiner Eignung als Kompetenzfeld für die Europäische Staatsanwaltschaft untersucht wird.[67]

I. Einführung: Die Europäische Staatsanwaltschaft

Seit dem Inkrafttreten des Vertrags von Lissabon sieht das EU-Primärrecht eine Kompetenz zur Weiterentwicklung von EUROJUST zu einer Europäischen Staatanwaltschaft vor. Nach Art. 86 Abs. 2 AEUV fiele dann „die strafrechtliche Untersuchung und Verfolgung sowie die Anklageerhebung […] vor den zuständigen Gerichten der Mitgliedstaaten" in deren Zuständigkeitsbereich.[68]

---

[63] Kap. 4 § 13 C. I. 1.
[64] Kap. 4 § 13 C. I. 2.
[65] Kap. 4 § 13 C. I. 3.
[66] Kap. 4 § 13 C. I. 4.
[67] Kap. 4 § 13 C. II.
[68] Für einen vertieften Einblick sei auf *Schramm*, JZ 2014, 749 ff., verwiesen, der die Notwendigkeit zur Errichtung, die Entstehungsgeschichte, praktische Herausforderungen und Perspektiven umfassend nachzeichnet.

1. Aufgabenbereich

Nachdem zunächst politische Studien[69] und wissenschaftliche Debattenbeiträge[70] zur Implementierung und Reichweite eines solchen neuen EU-Organs dominierten, hat die EU-Kommission Mitte 2013 einen ersten konkreten Vorschlag zur Einrichtung der EStA vorgelegt.[71] Das Primärrecht begrenzt durch Art. 86 Abs. 1 AEUV zwar den Kompetenzbereich einer zu gründenden EStA auf die „Bekämpfung von Straftaten zum Nachteil der finanziellen Interessen der Union". Schon im Vertrag von Lissabon ist allerdings die potenzielle Weiterentwicklung dieser neuen EU-Behörde bedacht worden, sodass deren Aufgabenbereich nach Art. 86 Abs. 4 AEUV „gleichzeitig mit der Annahme der Verordnung oder im Anschluss daran […] auf die Bekämpfung der schweren Kriminalität mit grenzüberschreitender Dimension" erweitert werden kann,[72] wenn die konkret verfolgte Straftat schwer ist und mehr als einen Mitgliedstaat betrifft.[73]

Damit ermöglicht das gültige EU-Primärrecht zwar nicht aktuell die Erstreckung der EStA-Kompetenzen auf die Bekämpfung der Computerkriminalität, statuiert aber eine sog. Kompetenzerweiterungsklausel, die im Rahmen eines vereinfachten Vertragsänderungsverfahrens abgerufen werden kann.[74] Eine Auseinandersetzung mit dieser Integrationsperspektive zum Computerstrafrecht der EU ist lohnenswert, da erstens Kompetenzausdehnungen für die EStA schon im Vertrag von Lissabon angelegt sind, zweitens Entwicklungen im EU-Recht bislang fast ausschließlich integrativ, also vertiefend, gewesen sind, sodass sich die hier dargestellten Perspektiven durchaus in das Harmonisierungsprogramm der EU einfügen und drittens, wie zu zeigen sein wird,[75] die

---

[69] Vgl. etwa die unter Leitung der Universität Luxemburg durchgeführten Vorstudien, deren Ergebnisse als *Ligeti*, Prosecutor for the European Union Bd. 1 und *Ligeti*, Prosecutor for the European Union Bd. 2 erschienen sind.

[70] Vgl. v. a. den sog. Corpus Juris von 1999/2000 als ersten konkreten Vorschlag zur Errichtung einer Europäischen Staatsanwaltschaft als überarbeitete Fassung bei *Delmas-Marty*, Implementation of the Corpus Juris; die ursprüngliche Fassung des Entwurfs in deutscher Übersetzung findet sich bei *Delmas-Marty*, Corpus Juris der strafrechtlichen Regelungen.

[71] Vorschlag für eine Verordnung des Rates über die Errichtung der Europäischen Staatsanwaltschaft, COM (2013) 534 final.

[72] Einen Überblick zum geschichtlichen Vorlauf bietet *Satzger*, NStZ 2013, 206 (207 f.) m. w. N.

[73] Intensiv mit den Voraussetzungen des Art. 86 Abs. 4 AEUV setzt sich *Rheinbay*, Die Errichtung einer Europäischen Staatsanwaltschaft, S. 113 ff., auseinander.

[74] Siehe zum Verfahren im Einzelnen *Vogel/Eisele*, in: Grabitz/Hilf/Nettesheim (Hrsg.), 57. EL Aug. 2015, Art. 86 AEUV Rn. 63 m. w. N.

[75] Siehe unten, Kap. 4 § 14 C. II.

Computerkriminalität einen optimalen Kriminalitätsbereich für eine solche Kompetenzerweiterung darstellt.

2. Institutioneller Aufbau

Dem Kommissionsvorschlag zufolge wird es sich bei der EStA um eine unabhängige Einrichtung der Union mit eigener Rechtspersönlichkeit handeln.[76] Nach dem vorgeschlagenen Modell wird die EStA einerseits zentral gesteuert, andererseits aber im jeweiligen Einzelfall dezentral tätig.[77] Dieser scheinbare Widerspruch liegt darin begründet, dass auf zentraler EU-Ebene ein gewählter EU-Staatsanwalt mit einer einmaligen Amtszeit von acht Jahren mit vier Stellvertretern und unterstützendem Personal eingesetzt werden soll. In den EU-Mitgliedstaaten wird es planmäßig zusätzlich abgeordnete EU-Staatsanwälte geben.[78] Diese sind dem EU-Staatsanwalt hierarchisch untergeordnet. Sie unterliegen allein seinen Weisungen und sind gänzlich unabhängig von den jeweiligen mitgliedstaatlichen Behörden, auch wenn sie zusätzlich in deren Organisationsstruktur eingebettet sind.[79]

3. Befugnisse

Bezüglich der Ermittlungs- und Beweiserhebungsbefugnisse der EStA lässt sich noch kein abschließendes Bild zeichnen. Zwar bietet Art. 26 VO-E Anhaltspunkte dahingehend, dass die EStA zum einen nach den mitgliedstaatlichen Prozessordnungen tätig wird, zum anderen aber gleichzeitig jenen Prozessordnungen gewisse Vorgaben für Mindeststandards bezüglich der eigenen Befugnisse macht. Jedoch sind viele prozessuale Fragen, etwa bezüglich der Beschuldigtenrechte, der grenzüberschreitenden Strafverteidigung, der transnationalen Beweiserhebung etc., weiterhin klärungsbedürftig. Für die vorliegende Untersuchung spielen diese Fragen allerdings lediglich eine untergeordnete Rolle, sodass insoweit auf die umfangreiche Literatur verwiesen wird.[80]

---

[76] Art. 3 Abs. 1, 2, Art. 5 Abs. 1, 2 VO-E.

[77] *Lohse*, in: Erkelens/Meij/Pawlik (Hrsg.), The European Public Prosecutor's Office, S. 165 (170); *Satzger*, NStZ 2013, 206 (207), spricht daher auch vom sog. gemischt national-supranationalen Modell; vgl. auch *Heger*, in: Giegerich (Hrsg.), Herausforderungen und Perspektiven der EU, S. 157 (163), der darauf hinweist, dass (zumindest nach dem aktuelen Primärrecht) etwaige EU-Staatsanwälte immer nur vor den nationalen Gerichten auftreten und Anklage erheben können.

[78] Art. 6 Abs. 1 bis 3, 5 VO-E; zu deren Wahlverfahren vgl. Art. 8 bis 11 VO-E.

[79] Siehe weiterführend zur geplanten Organisationsstruktur der Europäischen Staatsanwaltschaft *Esser*, StV 2014, 494 (496 ff.).

[80] Insbesondere mit den prozessualen Fragen einer Europäischen Staatsanwaltschaft

4. Aktueller Stand des Verfahrens

Der Zeitplan der EU zur Implementierung der EStA sah eigentlich deren Arbeitsaufnahme zum 1.1.2015 und die vollständige Funktionsfähigkeit bis 2023 mit 235 Bediensteten vor.[81] Vor allem nationale Bedenken hinsichtlich einer nicht ausreichenden demokratischen Kontrolle,[82] des beschränkten Aufgabenbereichs[83] sowie Vorbehalte gegen die Einflussnahme auf mitgliedstaatliches Strafprozessrecht[84] und die zentrale Organisationsform[85] der geplanten Behörde haben dazu geführt, dass die Arbeitsaufnahme bislang nicht erfolgen konnte.[86] Überdies wird vorgetragen, dass zunächst ein konkreter Katalog von Beschuldigtenrechten[87] festzuschreiben sowie eine internationale Verteidigerorganisation[88] zu implementieren sei, um eine effektive rechtliche Repräsentanz der Beschuldigten sicherstellen zu können.[89] Das Ziel einer vollumfänglichen staatsanwaltlichen Tätigkeit bis 2023 wird aber dennoch zunächst noch als realistisch eingeschätzt.[90] Letztlich hängen die Erfolgsaussichten und der weitere Zeitplan davon ab, wie schnell sich die Mitgliedstaaten auf einen abschließenden Verordnungsentwurf einigen können bzw. ob sich bei fehlender Einstimmigkeit genügend Staaten finden, die eine Europäische Staatsanwaltschaft zunächst im Wege der Verstärkten Zusammenarbeit errichten.[91]

Obgleich die politische Stimmung derzeitig nicht von einem besonderen Enthusiasmus für zusätzliche Harmonisierungsschritte und Kompetenzübertragungen von den Mitgliedstaaten auf die Europäische Union geprägt ist, gehen

---

auseinandergesetzt haben sich bislang u.a. *Esser*, StV 2014, 494 (502 ff.); *Grünewald*, HRRS 2013, 508 (511 ff.); *Ligeti/Simonato*, NJECL 2013, 7, 18 ff.

[81] COM (2013), 534 final, S. 9.

[82] *Erbežnik*, EuCLR 2015, 209 (214 f.).

[83] Ratsdok. 7095/14, Press Release, 3298th JHA-Counsil Meeting v. 3./4.3.2014, S. 16 f.

[84] Siehe etwa zur Problematik der Zentralität der Europäischen Staatsanwaltschaft ohne eigenes Prozessrecht *Grünewald*, HRRS 2013, 508 (515) m. w. N.

[85] Ratsdok. 7095/14, Press Release, 3298th JHA-Counsil Meeting v. 3./4.3.2014, S. 16 f.

[86] Weitere Fragen zur Legitimität einer Europäischen Staatsanwaltschaft werden von *Nieto Martin/Wade/Muñoz de Morales*, in: Ligeti (Hrsg.), Prosecutor for the European Union Bd. 1, S. 781 (787 ff.) aufgeworfen.

[87] Gemeinsame Stellungnahme der Bundesrechtsanwaltskammer (Nr. 22/2013) und des Deutschen Anwaltvereins (Nr. 48/2013) zum Vorschlag der Europäischen Kommission für eine Verordnung des Rates über die Errichtung der Europäischen Staatsanwaltschaft, S. 9; siehe auch *Zöller*, in: Böse (Hrsg.), EnzEuR Bd. 9, § 21 Rn. 100.

[88] *Asp u.a.* (Manifest Strafverfahrensrecht), ZIS 2013, 412 (422 f.); *Zöller*, in: Böse (Hrsg.), EnzEuR Bd. 9, § 21 Rn. 100.

[89] *Weißer*, in: Schulze/Zuleeg/Kadelbach (Hrsg.), Europarecht, § 42 Rn. 72.

[90] *Esser*, StV 2014, 494 (504).

[91] Siehe dazu *Zeder*, StraFo 2014, 239 (247 f.).

die Beratungen und Vorbereitungen hinsichtlich einer EU-Verordnung zur Errichtung der Europäischen Staatsanwalt unvermindert weiter.[92]

II. Computerstrafrecht als geeignete Rechtsmaterie für eine Erweiterung

Unabhängig davon, ob der Begriff der Computerkriminalität in Zukunft weiterhin als Sammelbegriff für alle in Verbindung mit einem Computer stehenden Straftaten verstanden wird[93] oder ob sich die hier vertretene, netzwerkspezifische Definition hinsichtlich Art. 83 Abs. 1 UAbs. 2 AEUV durchzusetzen vermag,[94] ist dieses Kriminalitätsfeld prädestiniert für eine Zuständigkeitserweiterung der zu gründenden Europäischen Staatsanwaltschaft.

Art. 86 Abs. 4 AEUV eröffnet, wie bereits erwähnt, entweder bereits mit Annahme der entsprechenden Verordnung oder jedenfalls im Nachgang die Möglichkeit zur „Ausdehnung der Befugnisse der Europäischen Staatsanwaltschaft auf die Bekämpfung der schweren Kriminalität mit grenzüberschreitender Dimension“. Sowohl der Begriff der schweren Kriminalität als auch jener der grenzüberschreitenden Dimension ist nicht legal definiert, sodass Inkongruenzen und Unbestimmtheiten kaum zu vermeiden sind. Es herrscht im Schrifttum und in der Kommentarliteratur jedoch insoweit Einigkeit, als dass zumindest die Kriminalitätsbereiche des Art. 83 Abs. 1 UAbs. 2 AEUV zum potenziellen Erweiterungskanon des Art. 86 Abs. 4 AEUV zu zählen sein dürften.[95] Jene Bereiche sind nämlich bereits als solche mit *besonders* schwerer Kriminalität mit grenzüberschreitender Dimension benannt. Da besonders schwere Kriminalität auch die schwere Kriminalität umfasst, ist somit lediglich fraglich, welche weiteren, *nur* schweren Kriminalitätsfelder zwar dem Zuständigkeitsbereich einer Europäischen Staatsanwaltschaft zuzurechnen, nicht jedoch im Rahmen von Art. 83 Abs. 1 AEUV materiell-rechtlich harmonisierungsfähig sind. Als in Art. 83 Abs. 1 UAbs. 2 AEUV explizit aufgeführter Kriminalitätsbereich ist die Computerkriminalität mithin grundsätzlich etwaigen Zuständigkeitserweiterungsambitionen zugänglich.

Auch unter Beachtung des EU-rechtlichen Subsidiaritätsprinzips nach Art. 5 Abs. 3 EUV, welchem insbesondere im Bereich des regelmäßig souveränitätsschonenden Strafrechts der EU eine wesentliche Rolle zufällt, kommt man zu keinem anderen Ergebnis. Eine Zuständigkeitserweiterung für die zu gründen-

---

[92] Eine aktuelle Dokumentation der Beratungen und Verodnungsentwürfe findet sich unter: http://db.eurocrim.org/db/de/vorgang/306/ (Stand: 07.08.2017).

[93] Siehe ausführlich bereits oben, Kap. 2 § 4.

[94] Siehe oben, Kap. 2 § 8 D. II.

[95] *Alexandrova*, in: Erkelens/Meij/Pawlik (Hrsg.), The European Public Prosecutor’s Office, S. 11 (18); *Dannecker*, in: Streinz (Hrsg.), Art. 86 AEUV Rn. 6; *Wasmeier/Killmann*, in: von der Groeben/Schwarze/Hatje (Hrsg.), Art. 86 AEUV Rn. 48.

de EStA verspricht eine bessere Eignung zur Bekämpfung der Computerkriminalität als die mitgliedstaatlichen Strafverfolgungsbehörden. Dafür sprechen zwei Erwägungen, die sich auf jeweils einen der Legitimationsgesichtspunkte für Harmonisierungen im Strafrecht der EU zurückführen lassen.

1. Bekämpfung transnationaler Kriminalitätserscheinungen

Die bestehenden Kooperationsmechanismen innerhalb der EU sind nicht hinreichend und supranationale Initiativen bezüglich einer strafrechtlichen Vollharmonisierung haben bislang eher utopischen Charakter, wie bereits aufgezeigt wurde. Gleichzeitig kann auf transnationale Sachverhalte durch lediglich nationalstaatlich legitimierte und agierende Strafverfolgungsbehörden nicht immer hinreichend reagiert werden. Mangelnde Ermittlungsmöglichkeiten sind dabei lediglich ein Teilaspekt, der in gewissem Umfang durch die Optimierung von polizeilicher und strafprozessualer Zusammenarbeit aufgefangen werden kann. Ein weiterer ist die sog. negative Mehrfachzuständigkeit, die in Verbindung mit dem EU-Doppelbestrafungsausschluss teilweise dazu führt, dass letztlich überhaupt kein Mitgliedstaat die Strafverfolgung übernimmt.[96] Um nämlich zu verhindern, dass Straftäter bei transnationalen Delikten in sämtlichen berührten Rechtsordnungen verurteilt werden können, gibt es in der EU durch Art. 50 GRC sowie Art. 54 SDÜ einen Doppelbestrafungsausschluss. Aus Kostengründen sind die einzelnen Behörden jetzt potenziell verleitet, auf ein Tätigwerden anderer Mitgliedstaaten zu vertrauen und in der Folge nicht selbstständig zu ermitteln.

Diese grundsätzlichen Vorteile einer EStA mit Befugnissen im Bereich der Computerkriminalitätsbekämpfung aus transnationaler Perspektive erkannte kürzlich auch *Brodowski*.[97] Derartige Erwägungen beziehen sich letztlich zu einem Großteil auf den Abbau von Reibungsverlusten durch die Zentralisierung von Strafverfolgungskompetenzen und die Verkürzung der behördlichen Reaktionszeit bei transnationalen Sachverhalten, indem Kooperationsmechanismen quasi „hochgezont" und dadurch europäisch institutionalisiert werden. Eine herausgehobene Stellung gegenüber den anderen Bereichen besonders schwerer Kriminalität mit grenzüberschreitender Dimension des Art. 83 Abs. 1 UAbs. 2 AEUV oder schwerer Kriminalität i. S. d. Art. 86 Abs. 4 AEUV nimmt die Computerkriminalität in diesem Kontext freilich nicht ein. Auch die anderen Kriminalitätsbereiche, wie Menschenhandel, illegaler Waffenhandel oder organisierte Kriminalität ließen sich durch eine europäische Strafverfolgungsbehörde möglicherweise effektiver bekämpfen, sodass die besondere Stellung des Computerkriminalitätsbereichs damit allein noch nicht nachgewiesen ist.

---

[96] *Brodowski*, in: Lange/Bötticher, Cyber-Sicherheit, S. 249 (259).

[97] *Brodowski*, in: Lange/Bötticher, Cyber-Sicherheit, S. 249 (268 ff.).

2. Schutz europäischer Rechtsgüter

Für den Bereich der Computerkriminalität bietet sich allerdings noch ein weiterer Ansatzpunkt zur Begründung an, um diese kooperativ-integrative Maßnahme auf EU-Ebene zu ergreifen.

Die oben gewonnene Erkenntnis,[98] dass IuK-Infrastrukturen als EU-Rechtsgüter anzuerkennen sind und damit Ähnlichkeiten mit den finanziellen Interessen der Union aufweisen, könnte eine EU-Behörde zum Schutz dieser Infrastrukturen auch mit strafrechtlichen Mitteln legitimieren. Nicht nur kann eine EStA schneller, flexibler und erfolgreicher transnationale Computerkriminalität bekämpfen, sondern sie würde darüber hinaus auch diejenige Ebene mit Strafverfolgungsbefugnissen ausstatten, deren Rechtsgüter vermehrt betroffen sind. Die europäischen IuK-Infrastrukturen sind den bislang erfolgten Richtlinien-Harmonisierungen zufolge besonders relevant für das Funktionieren des EU-Binnenmarktes[99] sowie des Raumes der Freiheit, der Sicherheit und des Rechts[100] und somit letztlich konstituierend für den EU-Verbund.

Als Hauptargument, zum Schutz der finanziellen Interessen der Union eine EU-Strafverfolgungsbehörde zu benötigen, wird regelmäßig ein nicht hinreichendes Interesse der Mitgliedstaaten zur Verfolgung von Straftaten, die *nur* die Union und nicht ihren eigenen nationalen Haushalt bedrohen, angeführt.[101] Dieser Ansatz trifft auf den Schutz von IuK-Infrastrukturen in vergleichbarer Weise zu. Zwar sind bei Angriffen auf Informationssysteme, die europäischen IuK-Infrastrukturen zuzurechnen sind, zumeist auch die jeweiligen mitgliedstaatlichen Infrastruktursysteme betroffen. Jedoch mögen die Auswirkungen im strafverfolgenden Mitgliedstaat nicht zwingend den europäischen Gegebenheiten Rechnung tragen. Die Relevanz eines Schadens kann mithin auf unionaler Ebene ungleich größer sein, als es für den einzelnen Mitgliedstaat zunächst erscheinen mag.

Beispiel: IT-Systeme sowie IuK-Infrastrukturen bringen es mit sich, dass Verletzungs- und Erfolgsort oftmals auseinanderfallen. Wenn also etwa der IuK-Knotenpunkt in Frankfurt angegriffen wird, können die Auswirkungen trotzdem zusätzlich oder gar ausschließlich bei der Energieversorgung in Lettland zu spüren sein.

---

[98] Siehe Kap. 4 § 13.

[99] Richtlinie 2013/40/EU, Erwägungsgrund 2.

[100] Richtlinie 2013/40/EU, Erwägungsgrund 3.

[101] Dahingehend die Begründung der Europäischen Kommission; COM (2013) 532 final, S. 3 f.; siehe auch die Ergebnisse der EuroNEEDs-Studie des Max-Planck-Instituts für ausländisches und internationales Strafrecht, 2011, S. 14 ff.; abrufbar unter: https://www.mpicc.de/files/pdf1/euroneeds_report_jan_2011.pdf (Stand: 07.08.2017).

Zunehmend sind durchaus wünschenswerte Entwicklungen in der EU dahingehend zu vernehmen, dass mehrfach vorhandene Infrastrukturen nur insoweit aufrechterhalten werden, als dies für die Gewährleistung der gemeinsamen Ziele notwendig ist. Der IuK-Knotenpunkt in Frankfurt nimmt daher beispielsweise nicht nur eine nationale Infrastrukturaufgabe wahr, sondern zusätzlich auch eine europäische.

Dieses Schicksal teilen sich die Schutzgüter der IuK-Infrastrukturen und der finanziellen Interessen der EU. Gefährdet sind jeweils nicht ausschließlich die Mitgliedstaaten, sondern zu einem Großteil auch die EU selbst, wenn entweder ihre Finanzmittel negativ beeinträchtigt oder europäische Infrastrukturen angegriffen werden.

Netzwerkspezifische Computerkriminalität lässt sich nicht nur effektiver auf europäischer als auf nationaler Ebene bekämpfen,[102] sondern bedroht mit den europäischen IuK-Infrastrukturen auch genuine EU-Rechtsgüter. Wie im Falle der finanziellen Interessen der EU ist es daher geboten, nicht auf hinreichende mitgliedstaatliche Strafverfolgungsinteressen zu vertrauen, sondern stattdessen die EU mit eigenen Ermittlungs- und Anklagebefugnissen auszustatten.

III. Umfang der Strafverfolgungsbefugnisse

Sollte gleichzeitig mit oder erst später nach erfolgreicher Errichtung einer EStA deren Zuständigkeitsbereich über die bislang geplante Strafverfolgungskompetenz hinsichtlich Delikten gegen die finanziellen Interessen der Union hinaus auch auf die Bekämpfung der Computerkriminalität ausgedehnt werden, stellt sich die Frage, in welcher Weise die EStA tätig würde. Einerseits wäre zu klären, welche strafprozessualen Ermittlungs- und Beweiserhebungsbefugnisse der neuen EU-Behörden zufielen. Obwohl Ermittlungen im Bereich der Computerkriminalität vielfach signifikante Besonderheiten gegenüber klassischen Deliktskategorien aufweisen, soll diese Frage hier offenbleiben, da derartige Fragestellungen noch nicht einmal für den zunächst ausschließlichen Aufgabenbereich der EStA hinreichend eindeutig sind.[103]

Andererseits wäre zu entscheiden, ob der EStA im Bereich der Computerkriminalität eine ausschließliche Strafverfolgungskompetenz zufallen sollte oder ob sie vielmehr ergänzend zu den mitgliedstaatlichen Staatsanwaltschaften tätig wird. Hinsichtlich der Verfolgung von Delikten gegen die finanziellen Interes-

---

[102] Selbstverständlich wäre eine enge Kooperation auf noch höherer internationaler Ebene ungleich wirkungsvoller, jedoch bietet allein das EU-Recht derzeitig eine Möglichkeit zur vertieften Integration, sodass im globalen Kontext zunächst weiterhin auf völkerrechtliche Konventionen und zwischenstaatliche Kooperationen gesetzt werden muss.

[103] Siehe oben, Kap. 4 § 14 C. 3.

sen der Union ist die Strafverfolgungskompetenz der EStA umfassend ausgestaltet. Das bedeutet, dass die EStA jeden Sachverhalt im Zusammenhang mit Delikten gegen die finanziellen Interessen der Union selbstständig ermitteln und zur Anklage bringen kann. Für diejenigen Deliktsbereiche, die der EStA erst durch den Zuständigkeitserweiterungsmechanismus des Art. 86 Abs. 4 S. 1 AEUV zufallen, stellt sich die Situation jedoch etwas anders dar. Hinsichtlich jener wird nämlich in Art. 86 Abs. 4 S. 1 a. E. AEUV als weitere Voraussetzung statuiert, dass nur Straftaten betroffen sind, die sich auf mindestens zwei Mitgliedstaaten beziehen. Rein nationale Sachverhaltskonstellationen können somit auch dann nicht in den Zuständigkeitsbereich der EStA fallen, wenn sie grundsätzlich einem transnationalen Kriminalitätsbereich unterfallen.

Aus diesen primärrechtlichen Vorgaben ergeben sich wiederum zwei Anschlussfragen. Erstens ist zu entscheiden, ob bei Vorliegen transnationaler Sachverhalte die ausschließliche oder lediglich eine zusätzliche Strafverfolgungszuständigkeit auf die EStA übergehen sollte. Zweitens könnte argumentiert werden, dass die europäischen IuK-Infrastrukturen den finanziellen Interessen der Union als EU-Rechtsgüter gleichzustellen wären und daher auf das zusätzliche Erfordernis der Transnationalität gem. Art. 86 Abs. 4 S. 1 a. E. AEUV zumindest dann zu verzichten wäre, wenn eine Computerstraftat gegen derartige Infrastrukturen verübt wird.

Bezüglich der Frage einer komplementären oder einer exklusiven Zuständigkeit ist *Brodowski* zuzustimmen und mithin die Komplementarität zu präferieren,[104] wobei allerdings nicht alle vier hierzu vorgetragenen Begründungen tragfähig sind. Er führt erstens an, dass es sich bei Computerstraftaten um Massenkriminalität handele, die sich nur mit einer komplementären Staatsanwaltsschafts-Infrastruktur sinnvoll bewältigen lasse. Zweitens seien die Mitgliedstaaten, im Gegensatz zu Delikten gegen die finanziellen Interessen der Union, bei der Computerkriminalität immer auch selbst an einer Aufklärung interessiert. Drittens würden durch eine ausschließliche Ausgestaltung weitreichende Parallelstrukturen geschaffen, die effektiven Strafverfolgungszielen nicht zuträglich sind und viertens könnten dieselben Erfolge auch durch eine verbesserte Koordination zwischen den jeweiligen nationalstaatlichen Staatsanwaltschaften erzielt werden. Während den Gründen 1 und 3 beizupflichten ist, kann von einem eigenen Interesse der Mitgliedstaaten bei der Bekämpfung der Computerkriminalität nicht ohne Weiteres ausgegangen werden.[105] Im Übrigen könnte diese Begründung in gleicher Weise gegen jede Form der materiellen Strafrechtsharmonisierung vorgetragen werden. Offensichtlich ist das Strafverfol-

---

[104] *Brodowski*, in: Lange/Bötticher (Hrsg.), Cyber-Sicherheit, S. 249 (270 f.).
[105] Siehe insoweit bereits die obige Argumentation in Kap. 3 § 11 E. II.

gungsinteresse allerdings nicht in allen Mitgliedstaaten auf gleichem Level, sodass EU-rechtliche Mindestvorschriften geboten sind, um ein entsprechendes Strafbarkeitsniveau herzustellen. Auch dem vierten Gesichtspunkt ist zu widersprechen, da nicht hinreichende Koordinations- und Kooperationsvorgänge trotz Bestehen entsprechender Institutionen, wie OLAF und EUROJUST, gerade der Auslöser für die Errichtung einer EStA sind.[106]

Die Befürchtungen, weitreichende Parallelstrukturen seien nicht geeignet, um strukturelle Defizite zu beheben, und die Beauftragung der EStA mit sämtlichen Computerdelikten würde jene überfordern, werden hingegen geteilt und sind für sich genommen ausreichend, um mit *Brodowski* eine komplementär und daher dem Internationalen Strafgerichtshof in vergleichbarer Weise agierende EStA im Bereich der Computerkriminalität zu bevorzugen.[107]

Abschließend bleibt noch die Frage zu klären, ob das Erfordernis der Transnationalität von Computerdelikten i. S. d. Art. 86 Abs. 4 S. 1 a. E. AEUV in jedem Fall notwendig ist, um eine Zuständigkeit der EStA zu begründen oder ob gegebenenfalls die Anerkennung und Betroffenheit von EU-Rechtsgütern eine Strafverfolgungskompetenz auch bei rein nationalen Computerstraftaten rechtfertigen könnte. Als EU-Rechtsgut sind bereits oben die kritischen digitalen Infrastrukturen innerhalb der Union identifiziert worden. Zwar werden die Sachverhalte, in denen jenes Rechtsgut geschädigt wird, ohne dass dabei mehrere Mitgliedstaaten betroffen sind, nicht zuletzt aufgrund der hiesigen Ausführungen zur Vernetzung, sehr selten sein, dennoch ist das Rechtsgut der kritischen europäischen IuK-Infrastrukturen qualitativ von den Rechtsgütern der anderen transnationalen Deliktsbereiche, die für eine Zuständigkeitserweiterung der EStA infrage kommen, zu unterscheiden. Nicht nur die transnationale Dimension ist hier Ansatzpunkt für die unionale Strafverfolgungskompetenz, sondern vor allem auch die Betroffenheit übergreifender und die Union in ihrem Bestand bedrohender Rechtsgüter.

Während die EU-weite Bekämpfung des Drogenhandels beispielsweise vornehmlich auf die Erleichterung von Maßnahmen über die Landesgrenzen hinweg zurückzuführen ist, bedroht ein Angriff des Frankfurter IT-Knotens die gesamte IuK-Infrastruktur (und damit als Meta-Infrastruktur potenziell auch alle anderen kritischen Infrastrukturen) der EU. Die Aufgabenerfüllung der Union bei der Gewährleistung eines Raumes der Freiheit, der Sicherheit und des Rechts sowie eines funktionierenden Binnenmarktes wäre kaum sicherzustellen.

---

[106] Siehe u. a. COM (2013) 532 final, S. 6.

[107] Vgl. *Brodowski*, in: Lange/Bötticher (Hrsg.), Cyber-Sicherheit, S. 249 (270 f.).

Somit sollten die kritischen IuK-Infrastrukturen der EU analog den finanziellen Interessen der EU nicht nur im Wege der transnationalen Kriminalitätsbekämpfung in den Zuständigkeitsbereich der EStA fallen, sondern vielmehr als genuine EU-Rechtsgüter anerkannt werden. Erstrebenswert wäre mithin eine komplementäre Strafverfolgungskompetenz der EStA für transnationale Sachverhalte innerhalb der Kriminalitätsbereiche des Art. 83 Abs. 1 UAbs. 2 AEUV und eine ausschließliche und umfassende Strafverfolgungskompetenz bei Straftaten gegen EU-Rechtsgüter. Man könnte also auch von einer Weiterentwicklung der sog. Euro-Crimes[108] des Art. 83 Abs. 1 UAbs. 2 AEUV zu genuinen EU-Rechtsgütern sprechen. Während die Euro-Crimes in materieller Hinsicht auf ein EU-weit vergleichbares Strafbarkeitsniveau und aus prozessualer Perspektive potenziell auf koordinierte EU-weite Ermittlungen und Anklagen gerichtet sind, um gemeinsame Werte innerhalb des europäischen Staatenverbundes zu definieren und zu verteidigen, zielt die Identifikation von EU-Rechtsgütern auf den Schutz der Union als solche ab.

Bezüglich der Ausschließlichkeit bzw. Komplementarität einer EStA-Zuständigkeit wäre mithin zwischen Euro-Crimes auf der einen und EU-Crimes auf der anderen Seite abzugrenzen.

Erstere umfassen die Bereiche des Art. 83 Abs. 1 UAbs. 2 AEUV und damit solche, die EU-weit zu verfolgen und zu bestrafen sind, da sie besonders schwere und grenzüberschreitende Kriminalität beinhalten, die überdies einen gemeinsamen strafrechtlichen Wertekanon innerhalb der EU andeutet.

Letztere hingegen betreffen, nach der hier vorgeschlagenen Definition, nicht zwingend transnationale Sachverhalte besonders schwerer Kriminalität. Vielmehr drückt sich die strafrechtlich relevante EU-Dimension dadurch aus, dass die Funktionsfähigkeit der Europäischen Union durch die jeweiligen Straftaten unmittelbar bedroht ist. Bereits kodifiziert ist diese Kategorie durch den Schutz der finanziellen Interessen der EU. Vorliegend wurde überdies der Schutz kritischer EU-IuK-Infrastrukturen als weiteres schützenswertes Rechtsgut herausgearbeitet. Wesentliche Bereiche einer funktionsfähigen Union sind dadurch abgedeckt, dass der strafrechtliche Schutz des EU-Haushalts und der EU-Meta-IuK-Infrastruktur in die Kompetenz des unmittelbar betroffenen Verfassungs-akteurs gelegt wäre. Freilich sind aber dennoch weitere derartige EU-Crimes denkbar, die sich beispielsweise im Kriminalitätsbereich des Terrorismus finden lassen könnten, wenn Institutionen und Einrichtungen der EU unmittelbar Opfer terroristischer Aktivitäten würden.

---

[108] Die Begriffsverwendung (deutsch: Europa-Delikte) findet sich u. a. bei *Samuli*, Criminal Law and Policy in the European Union, S. 145 ff., und bezieht sich auf die Kriminalitätsbereiche des Art. 83 Abs. 1 UAbs. 2 AEUV.

§ 15 Ergebnis zu den computerstrafrechtlichen Perspektiven in der EU

Um eine effektive Bekämpfung der Computerkriminalität innerhalb der Europäischen Union zu gewährleisten, sind über die materielle Harmonisierung durch Mindeststrafbarkeiten hinaus weitere Entwicklungsschritte erforderlich. Insbesondere der Schutz kritischer Infrastrukturen ist im vernetzten Europa signifikant. Da die IuK-Infrastrukturen nicht nur selbstständig schützenswert sind, sondern überdies auch vielfach die Grundbedingung zum Funktionieren anderer kritischer Infrastrukturen darstellen, ist ihr besonderer Schutz auch mit strafrechtlichen Mitteln geboten. Während koordinative Harmonisierungsmodelle als notwendig, aber nicht hinreichend und supranationale Harmonisierungsmodelle als zumindest derzeitig utopisch identifiziert worden sind, stellt das sog. hybride Harmonisierungsmodell mit seiner kooperativ angelegten Strafrechtsintegration unter maximaler Souveränitätswahrung die erforderlichen Maßnahmen bei gleichzeitiger realistischer Umsetzungswahrscheinlichkeit zur Verfügung.

Eine Zuständigkeitserweiterung der zu errichtenden Europäischen Staatsanwaltschaft auf die Bekämpfung der Computerkriminalität ermöglicht einerseits weiterhin die weitgehende strafrechtliche Eigenständigkeit der Mitgliedstaaten,[109] kann aber andererseits ebenfalls flexibel und koordiniert auf transnationale Computerstraftaten und Angriffe auf kritische IuK-Infrastrukturen der EU reagieren.

[109] Eine solche Eigenständigkeit ist insbesondere auch deshalb erstrebenswert, da nur in einem sog. Wettlauf der Rechtssysteme die notwendige rechtliche Innovationskraft aufrechterhalten werden kann; *Deakin*, ELJ 12 (2006), 440.

Fazit

Kaum ein Kriminalitätsphänomen verbreitet sich mit einer derartigen Geschwindigkeit wie die Computerkriminalität. Weder die empirische noch die normative Praxis und Forschung sind imstande, in hinreichender Geschwindigkeit politische, polizeiliche, rechtliche und wissenschaftliche Ergebnisse zur Bekämpfung derselben zu präsentieren. Nicht nur die immensen monetären Schadenssummen und die darüberhinausgehenden Schäden für Gesellschaften durch Angriffe auf kritische Infrastrukturen, sondern insbesondere auch die territoriale Schrankenlosigkeit des Internets sowie eine oftmals verminderte Hemmschwelle bei digitalen Angriffen – auch wenn real-weltliche Schäden angerichtet werden – stellen einzelne Länder, internationale Organisationen und die gesamte globale Staatengemeinschaft vor sich stetig erneuernde Herausforderungen.

Diese Arbeit konnte selbstverständlich nicht den Anspruch erheben, eine weltweit anwendbare und wirksame Computerkriminalitätsbekämpfungsstrategie zu entwickeln. Wie mehrfach aufgezeigt, ist ein Konsens der internationalen Staatengemeinschaft zum aktuellen Zeitpunkt noch nicht vorhanden. Nichtsdestotrotz reicht es teilweise immerhin zu regionalen und internationalen Kooperationsinitiativen,[1] die sich oftmals überdies nicht signifikant voneinander unterscheiden. Als erster überstaatlicher Zusammenschluss ist die Europäische Union hinsichtlich der verbundbasierten Computerkriminalitätsbekämpfung über lose zwischenstaatliche Kooperationsversprechen zur Verfolgungs- und Ermittlungsarbeit sowie nicht verbindliche völkerrechtliche Konventionen hinausgegangen. Seit dem Inkrafttreten des Vertrags von Lissabon im Jahre 2009 ist die Europäische Union gem. Art. 83 Abs. 1 UAbs. 2 AEUV befugt, EU-Richtlinien zur Angleichung von Straftaten und Strafen im Bereich der Computerkriminalität mit verbindlicher Wirkung für alle EU-Mitgliedstaaten zu erlassen. Diese weitreichende Rechtsintegration im strafrechtlichen Mehrebenensystem zwischen Union und Mitgliedstaaten kann vielen Herausforderun-

[1] *Jamil*, Council of Europe – Discussion Paper, S. 8, zeigt die unterschiedlichen Instrumente sowie deren jeweiligen Stärken und Schwächen bei der Nutzung als Modellgesetzgebung auf; abrufbar unter: https://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/2014/3021_model_law_study_v15.pdf (Stand: 07.08.2017).

gen des internationalen Computerstrafrechts begegnen; etwa indem verpflichtende Kriminalisierungsstandards und Zusammenarbeitserfordernisse begründet und gegebenenfalls auch durchgesetzt werden. Gleichzeitig schafft die Verlagerung strafrechtlicher Legislativkompetenzen grundsätzlich und insbesondere für den Bereich der Computerkriminalität vielfältige neue Problemfelder, die es im Rahmen dieser Arbeit zu beantworten galt.

In der weltweiten wissenschaftlichen Literatur und politischen Praxis wird der Begriff der Computerkriminalität – oder auch in seinen weiteren Erscheinungsformen als Cyber- oder Internetkriminalität – phänomenologisch bestimmt. Es wird somit regelmäßig keine klaren Begrenzung gesetzt, sondern lediglich ein kleinster gemeinsamer Nenner – jedwede Involvierung eines Computers im deliktischen Sachverhalt – gebildet, der letztlich statt einer Definition einen „basket of acts“[2] bildet. Für kriminologische Untersuchungen mag diese begriffliche Offenheit weniger hinderlich sein, die mit der unionsrechtlichen Verankerung verbundene Kompetenzübertragung durch die EU-Mitgliedstaaten auf den Unionsgesetzgeber erfordert aber einen zumindest bestimmbaren Computerkriminalitätsbegriff. Dieser hat den hergebrachten Rechtsgrundsätzen des politischen und normativen Mehrebenensystems der Europäischen Union sowie im strafrechtlichen Kontext insbesondere den Vertragszielen der Bekämpfung besonders schwerer und typischerweise grenzüberschreitender Kriminalität zu entsprechen. Somit kann Art. 83 Abs. 1 UAbs. 2 AEUV nach hier vertretener Auffassung nur dergestalt ausgelegt und interpretiert werden, dass allein der in dieser Arbeit entwickelte netzwerkspezifische Computerkriminalitätsbegriff zur unionalen Kompetenzbegründung heranzuziehen ist.

Auf der Harmonisierungskompetenz des Art. 83 Abs. 1 UAbs. 2 AEUV beruht bislang aus computerstrafrechtlicher Perspektive vor allem die Richtlinie über Angriffe auf Informationssysteme, die sich zumindest in Teilen als unionsrechtliche Ausgestaltung der Cybercrime Convention des Europarats verstehen lässt. Während die Rechtsharmonisierung in der Breite erfreulicherweise dem netzwerkspezifischen Computerkriminalitätsbegriff entspricht, gehen mit ihr jedoch durch die Regulierungstiefe verfassungs- und unionsrechtliche Probleme einher. Die flächendeckende Vorbereitungsstrafbarkeit bei Computerdelikten basiert freilich nicht lediglich auf dieser Richtlinie, wird allerdings erstmals unionsrechtlich und damit verbindlich perpetuiert. Zwar ist trotz dieser polizeilich-präventiven Instrumentalisierung des Strafrechts, durch die Möglichkeit, für die Mitgliedstaaten zum Schutz der nationalen Strafrechtsordnung das Notbremseverfahren nach Art. 83 Abs. 3 AEUV auszulösen, eine unionsrechtliche Nichtigkeit der Richtlinie nicht anzunehmen. Jedoch betreffen die entsprechen-

[2] *Sieber u. a.*, Comprehensive Study on Cybercrime, 2013, S. 12.

den Harmonisierungsvorgaben das Schuldprinzip sowie den *Ultima-Ratio*-Grundsatz und damit grundlegende Aspekte der deutschen Strafrechtsordnung. Dass dennoch von deutscher Seite die Möglichkeit eines Notbremseverfahrens außer Acht gelassen wurde, ist möglicherweise auf politische Opportunitätsgesichtspunkte zurückzuführen. Jedenfalls aber wirft dies Fragen hinsichtlich der Zweckmäßigkeit der innerstaatlichen Ausgestaltung des Notbremsemechanismus unter Einbeziehung der legislativen und exekutiven Gewalt, jedoch Auslassung der Judikative – mithin des Bundesverfassungsgerichts als Hüter der Verfassung – auf.

Schließlich hat sich gezeigt, dass auch im engen Bereich der netzwerkspezifischen Computerkriminalität zusätzliche Integrationsschritte in der Europäischen Union zu unternehmen sind, um insbesondere die kritischen IT-Infrastrukturen auch durch einen effektiven strafrechtlichen Schutz als Bestandteil eines umfangreichen Sicherheitskonzepts zu versehen. Die kritischen IT-Infrastrukturen sind nicht nur selbstständig schützenswert, sondern bezeichnen auch Meta-Infrastrukturen für fast sämtliche analoge kritische Infrastrukturen. Über diesen Rechtfertigungsansatz der Rechtsharmonisierung zur Bekämpfung transnationaler Kriminalitätserscheinungen hinaus stellen nach hier vertretener Auffassung die kritischen IT-Infrastrukturen durch die soeben genannte duale Schutzbedürftigkeit genuine EU-Rechtsgüter dar, die zukünftig als sog. EU-Crimes verfolgbar sein könnten. Dadurch eignet sich der netzwerkspezifische Computerkriminalitätsbereich als Erweiterungsfeld der in Gründung befindlichen Europäischen Staatsanwaltschaft gem. Art. 86 Abs. 4 AEUV.

Die Untersuchung hat somit viererlei gezeigt: Erstens ist die Europäische Union seit dem Inkrafttreten des Vertrags von Lissabon – zumindest auf dem europäischen Kontinent – durch die Möglichkeit der effektiven Rechtsharmonisierung der zukünftige Hauptakteur bei der Bekämpfung der Computerkriminalität. Zweitens erfordert die Kompetenz der Europäischen Union zur Richtlinienharmonisierung die Ausarbeitung eines Rechtsbegriffs der Computerkriminalität, der möglichweise in seiner Netzwerkspezifität liegen könnte. Drittens greifen aktuelle computerstrafrechtliche EU-Richtlinien auf ein Präventions- bzw. Risikostrafrecht zurück, dass sich kaum mit grundlegenden Aspekten der deutschen Strafrechtsordnung vereinbaren lässt und somit nationale Gegenmaßnahmen rechtfertigt, die freilich im Unionsrecht bereits vorgesehen sind. Viertens schließlich erfordern insbesondere die zunehmenden technologischen Abhängigkeiten innerhalb der Europäischen Union weitere Kooperationsinitiativen zur Bekämpfung und Verfolgung der netzwerkspezifischen Computerkriminalität, die etwa in einer Zuständigkeitserweiterung der in Gründung befindlichen Europäischen Staatsanwaltschaft liegen könnten.

Literaturverzeichnis

Abu-Zeitoun, Mamoun: Die Computerdelikte im deutschen Recht, Aachen 2005.

Albrecht, Michael: Die Kriminalisierung von Dual-Use Software, Berlin 2014.

Alexandrova, Vera: Presentation of the Commission's Proposal on the Establishment of the European Public Prosecutor's Office, in: Leendert Erkelens/Arjen Meij/Marta Pawlik (Hrsg.), The European Public Prosecutor's Office. An Extended Arm or a Two-Headed Dragon?, S. 11–20 (zitiert: *Alexandrova*, in: Erkelens/Meij/Pawlik (Hrsg.), The European Public Prosecutor's Office).

Ambos, Kai: Internationales Strafrecht, 4. Aufl. München 2014.

Ambos, Kai/Rackow, Peter: Erste Überlegungen zu den Konsequenzen des Lissabon-Urteils des Bundesverfassungsgerichts für das Europäische Strafrecht, ZIS 2009, S. 397–405.

Appazov, Artur: Legal Aspects of Cybersecurity, Kopenhagen 2014.

Appel, Ivo: Verfassung und Strafe. Zu den verfassungsrechtlichen Grenzen staatlichen Strafens, Berlin 1998.

Ashworth, Andrew/Horder, Jeremy: Principles of Criminal Law, 7. Aufl. Oxford 2013.

Asp, Petter/Bitzilekis, Nikolaos/Bogdan, Sergiu/Ziselholm, Thomas/Foffani, Luigi/Frände, Dan/Fuchs, Helmut/Kaiafa-Gbandi, Maria/Leblois-Happe, Jocelyne/Nieto, Martín Adán/Prittwitz, Cornelius/Satzger, Helmut/Symeonidou-Kastanidou, Elisabeth/Zerbes, Inge: Manifest zum Europäischen Strafverfahrensrecht, ZIS 2013, S. 412–429.

Asp, Petter/Bitzilekis, Nikolaos/Bogdan, Sergiu/Ziselholm, Thomas/Foffani, Luigi/Frände, Dan/Fuchs, Helmut/ Kaiafa-Gbandi, Maria /Leblois-Happe, Jocelyne/Nieto, Martín Adán/Prittwitz, Cornelius/Satzger, Helmut/Symeonidou-Kastanidou, Elisabeth/Zerbes, Inge: Manifest zur europäischen Kriminalpolitik, ZIS 2009, S. 697–706.

Bacigalupo, Enrique: Bemerkungen zu strafrechtlichen Fragen des Verfassungsentwurfs, ZStW 116 (2004), S. 326–330.

Bäcker, Matthias: Kriminalpräventionsrecht. Eine rechtsetzungsorientierte Studie zum Polizeirecht, zum Strafrecht und zum Strafverfahrensrecht, Tübingen 2015.

Bär, Wolfgang: Computerkriminalität, in: Heinz-Bernd Wabnitz/ders. (Hrsg.), Handbuch des Wirtschafts- und Steuerstrafrechts, 2. Aufl. München 2004, S. 801–886 (zitiert: *Bär*, in: Wabnitz/ders. (Hrsg.), Handbuch des Wirtschafts- und Steuerstrafrechts).

Barton, Dirk: Multimedia-Strafrecht. Ein Handbuch für die Praxis, Neuwied 1999.

Bassiouni, M. Cherif: International Criminal Law, Bd. 1: Crimes, 2. Aufl. Dobbs Ferry 1999.

Baumann, Jürgen/Weber, Ulrich/Mitsch, Wolfgang: Strafrecht: Allgemeiner Teil. Lehrbuch, 11. Aufl. Bielefeld 2003.

Beck, Wolfgang: Unrechtsbegründung und Vorfeldkriminalisierung. Zum Problem der Unrechtsbegründung im Bereich vorverlegter Strafbarkeit, - erörtert unter besonderer Berücksichtigung der Deliktstatbestände des politischen Strafrechts, Berlin 1992.

Beling, Ernst von: Die strafrechtliche Bedeutung der Exterritorialität. Beitrag zum Völkerrecht und zum Strafrecht, Breslau 1896.

Benoît-Rohmer, Florence: Das Recht des Europarats. Auf dem Weg zu einem pan-europäischen Rechtssystem, Berlin 2006.

Bergmann, Jan Michael (Hrsg.): Handlexikon der Europäischen Union, 5. Aufl. 2015 (zitiert: *Bearbeiter,* in: Bergmann (Hrsg.), Handlexikon der Europäischen Union).

Betzl, Karl Michael: Computerkriminalität – Dichtung und Wahrheit, DSWR 1972, S. 317–320.

Bieber, Klaus-Dieter: Rechtsprobleme des ec-Geldautomatensystems, WM 1987, Beilage Nr. 6, S. 3–31

Bieber, Roland/Epiney, Astrid/Haag, Marcel/Kotzur, Markus: Die Europäische Union. Europarecht und Politik, 12. Aufl. Baden-Baden 2016 (zitiert: *Bearbeiter*, in: Bieber et al. (Hrsg.), Europäische Union).

Böckenförde, Ernst-Wolfgang: Methoden der Verfassungsinterpretation. Bestandsaufnahme und Kritik, NJW 1976, S. 2089–2099.

Bogdandy, Armin von/Schill Stephan: Die Achtung der nationalen Identität unter dem reformierten Unionsvertrag, ZaöRV (70) 2010, S. 701–734.

Böhl, Meinrad/Reinhard, Wolfgang/Walter, Peter (Hrsg.): Hermeneutik. Die Geschichte der abendländischen Textauslegung von der Antike bis zur Gegenwart, Wien u. a. 2013 (zitiert: *Bearbeiter*, in: Böhl/Reinhard/Walter (Hrsg.), Hermeneutik).

Borchardt, Klaus-Dieter: Auslegung, Rechtsfortbildung und Rechtsschöpfung, in: Rainer Schulze/Manfred Zuleeg/Stefan Kadelbach (Hrsg.), Europarecht. Handbuch für die deutsche Rechtspraxis, 3. Aufl. Baden-Baden 2015, S. 625–642 (zitiert: *Borchardt*, in: Schulze/Zuleeg/Kadelbach (Hrsg.), Europarecht).

Borchardt, Klaus-Dieter: Die rechtlichen Grundlagen der Europäischen Union. Eine systematische Darstellung für Studium und Praxis, 6. Aufl. Wien 2015.

Borgers, Matthias: Functions and Aims of Harmonisation after the Lisbon Treaty. A European Perspective, in: Cyrille Fijnaut/Jannemeike Ouwerkerk (Hrsg.), The Future of Police and Judicial Cooperation in the European Union, Leiden 2012, S. 347–356 (zitiert: *Borgers*, in: Fijnaut/Ouwerkerk (Hrsg.), Police and Judicial Cooperation).

Borges, Georg/Stuckenberg, Carl-Friedrich/Wegener, Christoph: Bekämpfung der Computerkriminalität. Zum Entwurf eines Strafrechtsänderungsgesetzes zur Bekämpfung der Computerkriminalität, DuD 2007, S. 275–278.

Böse, Martin: Die Entscheidung des Bundesverfassungsgerichts zum Vertrag von Lissabon und ihre Bedeutung für die Europäisierung des Strafrechts, ZIS 2/2010, S. 76–91.

Böse, Martin: Grundrechte und Strafrecht als „Zwangsrecht", in: Roland Hefendehl/Andrew von Hirsch/Wolfgang Wohlers (Hrsg.), Die Rechtsgutstheorie. Legitimationsbasis des Strafrechts oder dogmatisches Glasperlenspiel?, Baden-Baden 2003, S. 89–95 (zitiert: *Böse*, in: Hefendehl/von Hirsch/Wohlers (Hrsg.), Rechtsgutstheorie).

Braum, Stefan: Europäisches Strafrecht im Fokus konfligierender Verfassungsmodelle. Stoppt das Bundesverfassungsgericht die europäische Strafrechtsentwicklung?, ZIS 8/2009, S. 418–426.

Brenner, Susan W.: Cybercrime and the Law. Challenges, Issues, and Outcomes, Boston 2012.

Breyer, Patrick: Die Cyber-Crime-Konvention des Europarats, DuD 2001, S. 592–600.

Broadhurst, Roderic/Chang, Yao-Chung: Cybercrime in Asia. Trends and Challenges, in: Jianhong Liu/Bill Hebenton/Susyan Jou (Hrsg.), Handbook of Asian Criminolohy, Berlin u. a. 2013, S. 49–63 (zitiert: *Broadhurst/Chang*, in: Liu/Hebenston/Jou (Hrsg.), Criminology).

Brodowski, Dominik: Cybersicherheit durch Cyber-Strafrecht. Über die strafrechtliche Regulierung des Internets, in: Hans-Jürgen Lange/Astrid Bötticher (Hrsg.), Cyber-Sicherheit, Wiesbaden 2015, S. 249–275 (zitiert: *Brodowski*, in: Lange/Bötticher (Hrsg.), Cyber-Sicherheit).

Brodowski, Dominik/Freiling, Felix C.: Cyberkriminalität, Computerstrafrecht und die digitale Scharrenwirtschaft, Berlin 2011.

Brunkhorst, Hauke: Die Legitimationskrise der Weltgesellschaft. Global Rule of Law, Global Constitutionalism und Weltstaatlichkeit, in: Mathias Albert/Rudolf Stichweh (Hrsg.), Weltstaat und Weltstaatlichkeit. Beobachtungen globaler politischer Strukturbildung, Wiesbaden 2007, S. 63–108 (zitiert: *Brunkhorst*, in: Albert/Stichweh (Hrsg.), Weltstaat und Weltstaatlichkeit).

Buck, Carsten: Über die Auslegungsmethoden des Gerichtshofs der Europäischen Gemeinschaft, Frankfurt a. M. u. a. 1998.

Bull, Hans Peter: Daseinsvorsorge im Wandel der Staatsformen, Der Staat 47 (2008), S. 1–19.

Bundesministerium des Innern: Nationale Strategie zum Schutz Kritischer Infrastrukturen (KRITIS-Strategie), abrufbar unter: http://www.bmi.bund.de/SharedDocs/Downloads/DE/Broschueren/2009/kritis.html (Stand: 21.3.2017).

Calliess, Christian/Ruffert, Matthias (Hrsg.): EUV, AEUV. Das Verfassungsrecht der Europäischen Union mit Europäischer Grundrechtecharta, 5. Aufl. München 2016 (zitiert: *Bearbeiter*, in: Calliess/Ruffert (Hrsg.).

Calliess, Christian: Die neue Europäische Union nach dem Vertrag von Lissabon: Ein Überblick über die Reformen unter Berücksichtigung ihrer Implikationen für das deutsche Recht, Tübingen 2010.

Calliess, Christian: Unter Karlsruher Totalaufsicht, FAZ vom 27. August 2009, abrufbar unter: http://www.faz.net/aktuell/politik/staat-und-recht/gastbeitrag-unter-karlsruher-total aufsicht-1845469.html (Stand: 21.3.2017).

Calliess, Christian: Auf dem Weg zu einem einheitlichen europäischen Strafrecht?, ZEuS 2008, S. 3–43.

Cappel, Alexander: Grenzen auf dem Weg zu einem europäischen Untreuestrafrecht: Das Mannesmann-Verfahren und § 266 StGB als Beispiele eines expansiven Wirtschaftsstrafrechts, Grundlagen gesamte Strafrechtswissenschaft, Bd. 4, Frankfurt a. M. u. a. 2009.

Chang, Yao-Chung: Cybercrime in the Greater China Region. Regulatory Responses and Crime Prevention across the Twaian Strait, Cheltenham 2012.

Chou, Yang-Yi: Zur Legitimation von Vorbereitungsdelikten, Baden-Baden 2011.

Clough, Jonathan: Principles of Cybercrime, Cambridge 2015.

Computer Crime Research Center: Putin Defies Convention on Cybercrime, abrufbar unter: http://www.crime-research.org/news/28.03.2008/3277 (Stand: 21.3.2017).

Constantinesco, Léontin-Jean: Die rechtsvergleichende Methode, Bd. 2, Köln u. a. 1972.

Dannecker, Gerhard: Das materielle Strafrecht im Spannungsfeld des Rechts der Europäischen Union, Teil I, JURA 2006, S. 95–102.

Danwitz, Thomas von: Rechtsschutz in der Europäischen Union, in: Armin Hatje/Peter-Christian Müller-Graff (Hrsg.), Enzyklopädie Europarecht. EnzEuR, Bd. 1: Europäisches Organisations- und Verfassungsrecht, Baden-Baden 2013, S. 747–794 (zitiert: *von Danwitz*, in: Hatje/Müller-Graff (Hrsg.), EnzEuR).

Deakin, Simon: Legal Diversity and Regulatory Competition: Which Model for Europe?, EJL 2006, S. 440–454.

Decocq, André/Montreuil, Jean/Buisson, Jacques: Le droit de la police, 2. Aufl. Paris 1998.

Delmas-Marty, Mireille/Vervaele, John A. E.: The Implementation of the Corpus Juris in the Member States, Antwerpen 2001.

Delmas-Marty, Mireille: Corpus Juris der strafrechtlichen Regelungen zum Schutz der finanziellen Interessen der Europäischen Union, Köln 1998.

Doehring, Karl: Die nationale „Identität" der Mitgliedsstaaten der Europäischen Union, in: Ole Due/Marcus Lutter/Jürgen Schwarze (Hrsg.), Festschrift für Ulrich Everling, Bd. 1, Baden-Baden 1995, S. 263–271 (zitiert: *Doehring*, in: FS Everling Bd. 1 (1995)).

Dorra, Fabian: Strafrechtliche Legislativkompetenzen der Europäischen Union. Eine Gegenüberstellung der Kompetenzlage vor und nach dem Vertrag von Lissabon, Baden-Baden 2013.

Dreier, Thomas/Schulze, Gernot (Hrsg.): Urheberrechtsgesetz. Urheberrechtswahrnehmungsgesetz, Kunsturhebergesetz. Kommentar, 5. Aufl. München 2015 (zitiert: *Bearbeiter*, in: Dreier/Schulze (Hrsg.), Urheberrechtsgesetz).

Dubber, Markus D./Hörnle, Tatjana (Hrsg.): The Oxford Handbook of Criminal Law, Oxford 2014.

Duttge, Gunnar: Vorbereitung eines Computerbetruges: Auf dem Weg zu einem „grenzenlosen" Strafrecht, in: Bernd Heinrich/Eric Hilgendorf/Wolfgang Mitsch/Detelv Sternberg-Lieben (Hrsg.), Festschrift für Ulrich Weber zum 70. Geburtstag, 18. September 2004, Bielefeld 2004, S. 285–310 (zitiert: *Duttge*, in: FS Weber (2004)).

Eisele, Jörg: Computer- und Medienstrafrecht, München 2013.

Ehmke, Horst: Prinzipien der Verfassungsinterpretation, VVDStRL 20 (1963), S. 53–102.

Erbežnik, Anže: European Public Prosecutor's Office (EPPO) – too much, too soon, and withou legitimacy, EuCLR 2015, S. 209–221.

Ernst, Stefan: Das neue Computerstrafrecht, NJW 2007, S. 2661–2666.

Eser, Albin: Internet und internationales Strafrecht, in: Dieter Leipold (Hrsg.), Rechtsfragen des Internet und der Informationsgesellschaft. Symposion der Rechtswissenschaftlichen Fakultäten der Albert-Ludwigs-Universität Freiburg und der Städtischen Universität Osaka, Heidelberg 2002, S. 303–326 (zitiert: *Eser*, in: Leipold (Hrsg.), Rechtsfragen des Internet und der Informationsgesellschaft).

Esser, Robert: Europäisches und Internationales Strafrecht, 2. Aufl. München 2014.

Esser, Robert: Die Europäische Staatsanwaltschaft: Eine Herausforderung für die Strafverteidigung, StV 2014, S. 494–504.

Esser, Robert: Befugnisse der europäischen Union auf dem Gebiet des Strafrecht?, in: Manfred Zuleeg (Hrsg.), Europa als Raum der Freiheit, der Sicherheit und des Rechts, Baden-Baden 2007, S. 25–46 (zitiert: *Esser*, in: Zuleeg (Hrsg.), Europa als Raum der Freiheit, der Sicherheit und des Rechts).

Europäische Kommission: Vorschlag für eine Verordnung des Rates über die Errichtung der Europäischen Staatsanwaltschaft, 17.07.2013, COM (2013) 534.

Europäische Kommission: Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen: Besserer Schutz der finanziellen Interessen der Union: Errichtung der Europäischen Staatsanwaltschaft und Reform von Eurojust, 17.07.2013, KOM (2013) 532.

Europäische Kommission: Mitteilung der Kommission an den Rat und das Europäische Parlament: Kriminalitätsbekämpfung im digitalen Zeitalter: Errichtung eines Europäischen Zentrums zur Bekämpfung der Cyberkriminalität, 28.03.2012, KOM (2012) 140.

Europäische Kommission: Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen: Eine Digitale Agenda für Europa, 19.05.2010, KOM (2010) 245.

Europäische Kommission: Mitteilung der Kommission an das Europäische Parlament, den Rat und den europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen: Ein Raum der Freiheit, der Sicherheit und des Rechts für die Bürger Europas. Aktionsplan zur Umsetzung des Stockholmer Programms, 20.04.2010, KOM (2010) 171.

Europäische Kommission: Vorschläge für eine Richtlinie des Europäischen Parlaments und des Rates zur Bekämpfung des sexuellen Missbrauchs und der sexuellen Ausbeutung von Kindern sowie der Kinderpornografie und zur Aufhebung des Rahmenbeschlusses 2004/68/JI des Rates, 29.03.2010, KOM (2010) 94.

Europäische Kommission: Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen über den Schutz kritischer Informationsinfrastrukturen: „Schutz Europas vor Cyber-Angriffen und Störungen großen Ausmaßes: Stärkung der Abwehrbereitschaft, Sicherheit und Stabilität", 30.03.2009, KOM (2009) 149.

Europäische Kommission: Mitteilung der Kommission an das Europäische Parlament, den Rat und den Ausschuss der Regionen: Eine allgemeine Politik zur Bekämpfung der Internetkriminalität, 22.05.2007, KOM (2007) 267.

Europäische Kommission: Mitteilung der Kommission: im Hinblick auf eine EU-Kinderrechtsstrategie, 04.07.2006, KOM (2006) 367.

Europäische Kommission: Mitteilung Strategische Ziele 2005–2009. Europa 2010 – Eine Partnerschaft für die Erneuerung Europas: Wohlstand, Solidarität und Sicherheit, 26.01.2005, KOM (2005) 12.

Europäische Kommission: Grünbuch über die Angleichung, die gegenseitige Anerkennung und die Vollstreckung strafrechtlicher Sanktionen in der Europäischen Union, 30.04.2004, KOM (2004) 334.

Europäische Kommission: Mitteilung der Kommission an das Europäische Parlament, den Rat und den europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen: Sicherheit der Netze und Informationen: Vorschlag für einen europäischen Politikansatz, 06.06.2001, KOM (2001) 298.

Europäische Kommission: Mitteilung der Kommission an das Europäische Parlament, den Rat und den europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen: Schaffung einer sichereren Informationsgesellschaft durch Verbesserung der Sicherheit von Informationsinfrastrukturen und Bekämpfung der Computerkriminalität, 21.01.2001, KOM (2000) 890.

Europäische Kommission: Mitteilung der Kommission an das Europäische Parlament, den Rat und den europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen: Illegale und schädigende Inhalte im Internet, 16.10.1996, KOM (1996) 487.

Europäische Kommission: Grünbuch über den Jugendschutz und den Schutz der Menschenwürde in den audio-visuellen und den Informationsmedien, 16.10.1996, KOM (1996) 483.

Europäische Kommission/Hohe Vertreterin der Europäischen Union für Außen- und Sicherheitspolitik: Gemeinsame Mitteilung an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen: Cybersicherheitsstrategie der Europäischen Union – ein offener, sicherer und geschützter Cyberraum, 07.02.2013, JOIN (2013) 1.

Everling, Ultricht: Richterliche Rechtsfortbildung in der Europäischen Gemeinschaft, JZ 2000, S. 217–227.

Fabio, Udo di: Der Verfassungsstaat in der Weltgesellschaft, Tübingen 2001.

Fahey, Elaine: The EU's Cybercrime and Cyber-Security Rulemaking. Mapping the Internal and External Dimensions of EU Security, European Journal of Risk Regulation 2014, S. 46–60.

Falliere, Nicolas/Murchu, Liam O./Chien, Eric: Stuxnet Dossier, Symantec Corp. Security Response, Cupertino 2011.

Fischer, Peter/Köck, Heribert Franz/Karollus, Margit Maria: Europarecht. Recht der EU, EG des Europarates und der wichtigsten anderen europäischen Organisationen, 4. Aufl. Wien 2002.

Fischer, Thomas: Strafgesetzbuch mit Nebengesetzen, 64. Aufl. München 2017.

Fletcher, Maria/Lööf, Robin/Gilmore, Bill: EU Criminal Law and Justice, Cheltenham 2008.

Frister, Helmut: Strafrecht Allgemeiner Teil. Ein Studienbuch, 7. Aufl. München 2015.

Funke, Andreas: Der Anwendungsvorrang des Gemeinschaftsrechts. Einige Problemfälle und ein Präzisierungsvorschlag, DÖV 2007, S. 733–740.

Gärditz, Klaus F.: Europäisierung des Strafrechts und nationales Verfassungsrecht, in: Martin Böse/Armin Hatje (Hrsg.), Enzyklopädie Europarecht. EnzEuR, Bd. 9: Europäisches Strafrecht. Mit polizeilicher Zusammenarbeit, Baden-Baden 2013, S. 227–268 (zitiert: *Gärditz*, in: Böse/Hatje (Hrsg.), EnzEuR).

Gärditz, Klaus F./Gusy, Christoph: Zur Wirkung europäischer Rahmenbeschlüsse im innerstaatlichen Recht. Zugleich Besprechung von EuGH, Urteil vom 16.06.2005, GA 2006, S. 225–237.

Gärditz, Klaus F.: Strafprozeß und Prävention. Entwurf einer verfassungsrechtlichen Zuständigkeits- und Funktionenordnung, Tübingen 2003.

Geiger, Robert: Auswirkungen europäischer Strafrechtsharmonisierung auf nationaler Ebene. Eine rechtsvergleichende Untersuchung am Beispiel des Rahmenbeschlusses 2004/68/JI zur Bekämpfung der sexuellen Ausbeutung von Kindern und der Kinderpornographie, Berlin 2012.

Geiger, Rudolf/Khan, Daniel-Erasmus/Kotzur, Markus (Hrsg.): EUV/AEUV. Vertrag über die Europäische Union und Vertrag über die Arbeitsweise der Europäischen Union, 6. Aufl. München 2017 (zitiert: *Bearbeiter*, in: Geiger/Khan/Kotzur (Hrsg.)).

Geppert, Klaus: Gefährdung des Straßenverkehrs (§ 315c StGB) und Trunkenheit im Straßenverkehr (§ 316 StGB), JURA 2001, S. 559–567.

Gercke, Björn: Straftaten und Strafverfolgung im Internet, GA 2012, S. 474–490.

Gercke, Marco: Die Entwicklung des Internetstrafrechts 2011/2012, ZUM 2012, S. 625–635.

Gercke, Marco: Understanding Cybercrime: Phenomena, Challenges and Legal Responses, September 2012, abrufbar unter: http://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf (Stand: 07.08.2017).

Gercke, Marco: 10 Years Convention on Cybercrime, Cri 2011, S. 142–149.

Gercke, Marco: The Globalization of Crime (UNDOC), 2010, abrufbar unter: http://www.unodc.org/documents/data-and-analysis/tocta/TOCTA_Report_2010_low_res.pdf (Stand: 07.08.2017).

Gercke, Marco/Brunst, Phillip W.: Praxishandbuch Internetstrafrecht, Stuttgart 2009.

Gercke, Marco/Tropina, Tatiana: From Telecommunication Standardisation to Cybercrime Harmonisation?, Cri 2009, S. 136–140.

Gern, Alfons: Die Rangfolge der Auslegungsmethoden von Rechtsnormen, VerwaltungsArchiv 80 (1989), S. 415–436.

Goldberg, Mark: From Latvia, without Love. EU-US Cybercrime Extradition in the Global Rights Conversation, CJEL 2014, S. 329–352.

Goodman, Marc D./Brenner, Susan W.: The Emerging Consensus on Criminal Conduct in Cyberspace, International Journal of Law and Information Technology 2002, S. 139–223.

Gordon, Sarah/Ford, Richard: On the Definition and Classification of Cybercrime, Journal in Computer Virology, 2006, S. 13–20.

Grabitz, Eberhard/Hilf, Meinhard/Nettesheim, Martin (Hrsg.): Das Recht der Europäischen Union, München 2015, Stand: 57. Erg.-Lfg. August 2015 (zitiert: *Bearbeiter*, in: Grabitz/Hilf/Nettesheim (Hrsg.)).

Grabitz, Eberhard: Gemeinschaftsrecht bricht nationales Recht, Hamburg 1966.

Graul, Eva: Abstrakte Gefährdungsdelikte und Präsumtionen im Strafrecht, Berlin 1991.

Greathouse, Craig B.: Cyber War and Strategic Thought: Do the Classic Theorists Still Matter?, in: Jan-Frederik Kremer/Benedikt Müller (Hrsg.), Cyberspace and International Relations. Theory, Prospects and Challenges, Berlin u. a. 2014, S. 21–40 (zitiert: *Greathouse*, in: Kremer/Müller (Hrsg.), Cyberspace).

Greve, Holger: Kritische Infrastrukturen, DuD 2009, S. 756–758.

Groeben, Hans von der/Schwarze, Jürgen/Hatje, Armin (Hrsg.): Europäisches Unionsrecht. Vertrag über die Europäische Union, Vertrag über die Arbeitsweise der Europäischen Union, Charta der Grundrechte der Europäischen Union, 7. Aufl. Baden-Baden 2015 (zitiert: *Bearbeiter*, in: von der Groeben/Schwarze/Hatje (Hrsg.)).

Groeben, Hans von der: Handbuch des europäischen Rechts. Systematische Sammlung mit Erläuterungen, Baden-Baden, Stand: 250. Lfg. Januar 2004.

Gröseling, Nadine/Höfinger, Frank Michael: Hacking und Computerspionage. Auswirkungen des 41. StrÄndG zur Bekämpfung der Computerkriminalität, MMR 2007, S. 549–553.

Gröseling, Nadine/Höfinger, Frank Michael: Computersabotage und Vorfeldkriminalisierung. Auswirkungen des 41. StrÄndG zur Bekämpfung der Computerkriminalität, MMR 2007, S. 626–630.

Grünewald, Annette: Eine Europäische Staatsanwaltschaft nach den Vorstellungen der Europäischen Kommission, HRRS 2013, S. 508–515.

Grünewald, Annette: Zur Frage eines europäischen Allgemeinen Teils des Strafrechts, JZ 2011, S. 972–977.

Grupp, Walter G./Schäder, Gerhard: Neue Tendenzen in der Rechtsprechung des Europäischen Gerichtshofes zur Verhältnismäßigkeit, EWS 1993, S. 27–29.

Haase, Adrian: Strafbewehrte Vorfeldhandlungen im Sicherheitsrecht – Computerstrafrecht jenseits von Rechtsgüterschutz und *Ultima Ratio*?, in: Christoph Gusy/ Dieter Kugelmann/ Thomas Würtenberger (Hrsg.): Rechtshandbuch Zivile Sicherheit, Berlin/Heidelberg 2017, S. 517–526 (zitiert: *Haase*, in: Gusy/Kugelmann/Würtenberger (Hrsg.), Zivile Sicherheit).

Haase, Adrian: Harmonizing Substantive Cybercrime Law through European Union Directive 2013/40/EU – From European Legislation to International Model Law?, IEEE Xplore Digital Library, ICACC 2015, S. 1–6.

Haase, Adrian: Kongressbericht: Cyberkriminalität als internationale Herausforderung. Thirteenth United Nations Congress on Crime Prevention and Criminal Justice vom 12.04. – 19.04.2015 in Doha, Katar, ZIS 7–8/2015, S. 422–425.

Häberle, Peter/Kotzur, Markus: Europäische Verfassungslehre, 8. Aufl. Baden-Baden 2016.

Hahn, Jörg-Uwe: Die Mitwirkungsrechte von Bundestag und Bundesrat in EU-Angelegenheiten nach dem neuen Integrationsverwantwortungsgesetz, EuZW 2009, S. 748–763.

Hahn-Lorber, Marcus: Are There Methods of Reasoning on ‚Meta-Legislation'? The Interpretation of Legislative Competence Norms within the Methodology of European Constitutional Law, ELJ 2010, S. 760–779.

Hale, Chris: Cybercrime: Facts & Figures Concerning this Global Dilemma, Crime and Justice International, 2002, Vol. 18, S. 24–26.

Haltern, Ulrich R.: Rechtswissenschaft als Europawissenschaft, in: Gunnar Folke Schuppert/ Ingolf Pernice/Ulrich R. Haltern (Hrsg.), Europawissenschaft, Baden-Baden 2005, S. 37–88 (zitiert: *Haltern*, in: Schuppert/Pernice/ders. (Hrsg.), Europawissenschaft).

Harding, Christopher: Forging the European Cartel Offence: The Supranational Regulation of Business Conspiracy, European Journal of Crime, Criminal Law and Criminal Justice 2004, S. 275–300.

Harley, Brian: A Global Convention on Cybercrime?, Columbia Science and Technology Law Review, XI, 2013, abrufbar unter: http://www.stlr.org/2010/03/a-global-convention-on-cybercrime/ (Stand: 07.08.2017).

Harms, Monika: Zur Europäisierung des Strafrechts – Europäisches Recht und materielles Strafrecht, in: Juristische Studiengesellschaft Karlsruhe (Hrsg.), Jahresband 2007, S. 173–192 (zitiert: *Harms*, in: Juristische Studiengesellschaft Karlsruhe (Hrsg.), Jahresband 2007).

Hart, Paul de/González Fuster, Gloria/Koops, Bert-Jaap: Fighting Cybercrime in the two Europes, Revue internationale de droit pénal, (77) 2006, S. 503–524.

Hassemer, Winfried: Sicherheit durch Strafrecht, StV 2006, S. 321–331.

Hassemer, Winfried: Theorie und Soziologie des Verbrechens. Ansätze zu einer praxisorientierten Rechtsgutslehre, Frankfurt a. M. 1973.

Hassold, Gerhard: Strukturen der Gesetzesauslegung, in: Claus-Wilhelm Canaris (Hrsg.), Festschrift für Karl Larenz zum 80. Geburtstag am 23. April 1983, München 1983, S. 211–240 (zitiert: *Hassold*, in: FS Larenz II (1983)).

Hatje, Armin/Mankowski, Peter: „Nationale Unionsrechte“ – Sprachgrenzen, Traditionsgrenzen, Systemgrenzen, Denkgrenzen, EuR 2014, S. 155–170.

Hay, Peter: US-Amerikanisches Recht. Ein Studienbuch, 6. Aufl. München 2015.

Hecker, Bernd: Europäisches Strafrecht, Heidelberg 2012.

Hecker, Bernd: Europäisches Strafrecht post-Lissabon, in: Kai Ambos (Hrsg.), Europäisches Strafrecht post-Lissabon, Göttingen 2011, S. 13–28 (zitiert: *Hecker*, in: Ambos (Hrsg.), Europäisches Strafrecht post-Lissabon).

Hefendehl, Roland: Die Rechtsgutslehre und der Besondere Teil des Strafrechts. Ein dogmatisch-empirischer Vergleich von Chile, Deutschland und Spanien, ZIS 2012, S. 506–512.

Hefendehl, Roland: in: ders. (Hrsg.), Grenzenlose Vorverlagerung des Strafrecht?, Berlin 2010, S. 89–108 (zitiert: *Hefendehl*, in ders. (Hrsg.), Grenzenlose Vorverlagerung).

Heger, Martin: Rechtsraum Europa – Zur Anpassung der Rechtssysteme im Strafrecht, RuP 2012, S. 88–96.

Heger, Martin: Europäisches Straf- und Strafverfahrensrecht, in: Thomas Giegerich (Hrsg.), Herausforderungen und Perspektiven der EU, Berlin 2012, S. 157–193 (zitiert: *Heger,* in: Giegerich (Hrsg.), Herausforderungen und Perspektiven der EU).

Heger, Martin: Die Europäisierung des deutschen Umweltstrafrechts, Tübingen 2009.

Heger, Martin: Perspektiven des Europäischen Strafrechts nach dem Vertrag von Lissabon. Eine Durchsicht des (wohl) kommenden EU-Primärrechts vor dem Hintergrund des Lissabon-Urteils des BVerfG vom 30.6.2009, ZIS 2009, S. 406–417.

Heger, Martin: Europäische Beweissicherung – Perspektiven der strafrechtlichen Zusammenarbeit in Europa, ZIS 2007, S. 547–556.

Heid, Daniela A.: Das tschechische Polizeirecht im Vergleich mit „europäischem Polizeirecht“ unter besonderer Berücksichtigung der Schengener Abkommen, Würzburg 2002.

Heinrich, Bernd: Zur Notwendigkeit der Unterscheidung von Amtsträgern und Mandatsträgern bei der Gestaltung der strafrechtlichen Korruptionstatbestände, ZIS 2016, S. 382–395.

Heinrich, Bernd: Strafrecht Allgemeiner Teil, 5. Aufl. Stuttgart 2016.

Heinrich, Bernd: Die Grenzen des Strafrechts bei der Gefahrprävention. Brauchen oder haben wir ein „ Feindstrafrecht“?, ZStW 121 (2009), S. 94–130.

Heinrich, Bernd: Handlung und Erfolg bei Distanzdelikten, in: ders./Eric Hilgendorf/Wolfgang Mitsch/Detlev Sternberg-Lieben (Hrsg.), Festschrift für Ulrich Weber zum 70. Geburtstag, 18. September 2004, Bielefeld 2004, S. 91–108 (zitiert: *Heinrich*, in: FS Weber (2004)).

Heintschel-Heinegg, Bernd von (Hrsg.): Beck'scher Online-Kommentar StGB, 33. Ed. Stand: 01.12.2016, München 2017 (zitiert: *Bearbeiter*, in: Beck-OK StGB).

Heinz, Wolfang: Der strafrechtliche Schutz des kartengestützten Zahlungsverkehrs, in: Max-Emanuel Geis/Dieter Lorenz (Hrsg.), Staat, Kirche, Verwaltung. Festschrift für Hartmut Maurer zum 70. Geburtstag, München 2001, S. 1111–1136 (zitiert: *Heinz*, in: FS Maurer (2001)).

Hentschel, Peter/König, Peter/Dauer, Peter (Hrsg.): Straßenverkehrsrecht, 43. Aufl. München 2015.

Herdegen, Matthias: Europarecht, 17. Aufl. München 2015.

Herlin-Karnell, Ester: The Constitutional Dimension of European Criminal Law, Oxford 2012.

Herrmann, Christoph: Richtlinienumsetzung durch die Rechtsprechung, Berlin 2003.

Hesse, Konrad: Verfassungsrechtsprechung im geschichtlichen Wandel, JZ 1995, S. 265–273.

Hilgendorf, Eric/Valerius, Brian: Computer- und Internetstrafrecht. Ein Grundriss, 2. Aufl. Berlin 2012.

Hilgendorf, Eric: Die neuen Medien und das Strafrecht, ZStW 113 (2001), S. 650–680.

Hinrichs, Fabian: Das Recht der spanischen Vollzugspolizei, Würzburg 2004.

Hirsch, Hans Joachim: Internationalisierung des Strafrechts und Strafrechtswissenschaft: Nationale und universale Strafrechtswissenschaft, ZStW 116 (2005), S. 835–854.

Hirsnik, Erkki: Die Strafbarkeit eines Angriffs auf das Computersystem nach deutschem, estnischem, europäischem und internationalem Recht, Hamburg 2013.

Hobe, Stephan: Europarecht, 8. Aufl. München 2014.

Hoeren, Thomas: Internetrecht, Münster 2016, Stand: April 2016.

Höfinger, Frank Michael: Anmerkung zu BVerfG, Beschluss vom 18. Mai 2009 – 2 BvR 2233/07, ZUM 2009, S. 751–753.

Holznagel, Bernd (Hrsg.): IT-Sicherheit in der Informationsgesellschaft – Schutz kritischer Infrastrukturen, Münster 2001.

Hörnle, Tatjana: Deskriptive und normative Dimensionen des Begriffs „Feindstrafrecht“, GA 2006, S 80–95.

Husemann, Stephan: Die Verbesserung des strafrechtlichen Schutzes des bargeldlosen Zahlungsverkehrs durch das 35. Strafrechtsänderungsgesetz, NJW 2004, S. 104–109.

Iglesias, Gil Carlos Rodriguez: Perspektiven europäischer und nationaler Verfassungsgerichtsbarkeit im Lichte des Vertrags über eine Verfassung für Europa, in: Walter-Hallstein-Institut für Europa (Hrsg.), Europäische Verfassung in der Krise – auf der Suche nach einer gemeinsamen Basis für die erweiterte Europäische Union, Forum Constitutionis Europae, Bd. 7, Baden-Baden 2007, S. 107–118 (zitiert: *Iglesias*, in: Walter-Hallstein-Institut für Europa (Hrsg.), Europäische Verfassung in der Krise).

Inglis, Kirstyn: EU Environmental Law and its Green Footprints in the World, in: Alan Dashwood (Hrsg.), Law and Practice of EU External Relations, Cambridge 2009, S. 429–464 (zitiert: *Inglis*, in: Dashwood (Hrsg.), EU external relations).

International Military Tribunal: Der Prozess gegen die Hauptkriegsverbrecher vor dem Internationalen Militärgerichtshof. Nürnberg, 14. November 1945 – 1. Oktober 1946, Nürnberg 1947.

Intven, Hank/Pfohl, Richard/Slusarchuk, Cheryl/Sookman, Barry: The World Bank Legal Review: Law and Justice for Development, Vol. 1, Washington D.C. 2003.

Ipsen, Knut (Hrsg.): Völkerrecht. Ein Studienbuch, 6. Aufl. München 2014 (zitiert: *Bearbeiter*, in: Ipsen (Hrsg.), Völkerrecht).

Isensee, Josef/Kirchhof, Paul (Hrsg.): Handbuch des Staatsrechts, 3. Aufl. 2005 (zitiert: *Bearbeiter*, in: Isensee/Kirchhof (Hrsg.), Handbuch des Staatsrechts).

Jakobs, Günther: Rechtsgüterschutz? Zur Legitimation des Strafrechts, 538. Sitzung am 5. September 2012 in Düsseldorf, Vorträge Nordrhein-Westfälische Akademie der Wissenschaften und der Künste 440, Paderborn u. a. 2012.

Jamil, Zahid: Cybercrime Model Laws, Council of Europe – Discussion Paper, 2014, S. 1–38, abrufbar unter: https://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/2014/3021_model_law_study_v15.pdf (Stand: 07.08.2017).

Jellinek, Walter: Allgemeine Staatslehre, 3. Aufl. Berlin 1914.

Jescheck, Hans-Heinrich/Weigend, Thomas: Lehrbuch des Strafrechts. Allgemeiner Teil, 5. Aufl. Berlin 1996.

Jescheck, Hans-Heinrich: Die Strafgewalt übernationaler Gemeinschaften, ZStW 65 (1953), S. 496–518.

Joecks, Wolfgang (Hrsg): Münchener Kommentar zum Strafgesetzbuch, 2. Aufl. München 2012 (zitiert: *Bearbeiter*, in: MüKo-StGB).

Jones, Christopher: Mobile internetfähige Geräte im Strafrecht, Berlin 2014.

Kaiafa-Gbandi, Maria: The Importance of Core Principles of Substantive Criminal Law for a European Criminal Policy Respecting Fundamental Rights and the Rule of Law, EuCLR 2011, S. 6–33.

Kaiafa-Gbandi, Maria: Aktuelle Strafrechtsentwicklung in der EU und rechtsstaatliche Defizite, ZIS 11/2006, S. 521–536.

Kaspar, Johannes: Verhältnismäßigkeit und Grundrechtsschutz im Präventionsstrafrecht, Baden-Baden 2014.

Kaufmann, Armin: Die Aufgabe des Strafrechts, Wiesbaden 1983.

Kindhäuser, Urs: Strafe, Strafrechtsgut und Rechtsgüterschutz, in: Klaus Lüderssen u. a. (Hrsg.), Modernes Strafrecht und Ultima-ratio-Prinzip, Frankfurt a. M., 1990, S. 29–38 (zitiert: *Kindhäuser*, in: Lüderssen u. a. (Hrsg.), Modernes Strafrecht).

Kindhäuser, Urs/Neumann, Ulfrid/Paeffgen, Hans-Ullrich (Hrsg.): Strafgesetzbuch, 4. Aufl. Baden-Baden 2013 (zitiert: *Bearbeiter*, in: NK-StGB).

Kindhäuser, Urs: Gefährdung als Straftat. Rechtstheoretische Untersuchungen zur Dogmatik der abstrakten und konkreten Gefährdungsdelikte, Frankfurt a. M. 1989.

Kirsch, Andrea: Demokratie und Legitimation in der Europäischen Union, Baden-Baden 2008.

Klesczewski, Diethelm: Strafrecht. Allgemeiner Teil, Leipzig 2012.

Kleve, Pieter/De Mulder, Richard/van Noortwijk, Kees: The Definition of ICT Crime, in: Sylvia Kierkegaard/Patrick Kierkegaard (Hrsg.), Private Law: Right, Duties & Conflicts, International Association of IT Lawyers, 2010, S. 56–66 (zitiert: *Kleve/Mulder/Noortwijk*, in: S. Kierkegaard/P. Kierkegaard (Hrsg.), Rights, duties & conflicts).

Klimek, Libor: European Arrest Warrant, Heidelberg u. a. 2015.
Klip, André: European Criminal Law, 2. Aufl. Cambridge 2012.
Klip, André: Strafrecht in der Europäischen Union, ZStW 117 (2005), S. 889–911.
Koch, Hans-Joachim/Rüßmann, Helmut: Juristische Begründungslehre. Eine Einführung in Grundprobleme der Rechtswissenschaft, München 1982.
Kochheim, Dieter: Cybercrime und Strafrecht in der Informations- und Kommunikationstechnik, München 2015.
Köhler, Michael: Strafrecht. Allgemeiner Teil, Berlin u. a. 1997.
Kolz, Harald: Zur Aktualität der Bekämpfung der Wirtschaftskriminalität für die Wirtschaft, wistra 1982, S. 167–172.
König, Wolfgang/Popescu-Zeletin, Radu/Schliesky, Utz: IT und Internet als kritische Infrastruktur: vernetzte Sicherheit zum Schutz kritischer Infrastrukturen, Kiel 2014.
Koops, Bert-Jaap: The Internet and its Opportunities for Cybercrime, Transnational Criminology Manual, 2010, Vol. 1, S. 735–754.
Koriath, Heinz: Zum Streit um die Gefährdungsdelikte, GA 2001, S. 51–74.
Krey, Volker/Esser, Robert: Deutsches Strafrecht. Allgemeiner Teil, 6. Aufl. Stuttgart 2016.
Krischker, Sven: Das Strafrecht vor neuen Herausforderungen, Berlin 2014.
Kugelmann, Dieter: Europäische Polizeiliche Kooperation, in: Martin Böse/Armin Hatje (Hrsg.), Enzyklopädie Europarecht. EnzEuR, Bd. 9: Europäisches Strafrecht. Mit polizeilicher Zusammenarbeit, Baden-Baden 2013, S. 631–678 (zitiert: *Kugelmann*, in: Böse/Hatje (Hrsg.), EnzEuR).
Kutscher, Hans: Gerichtshof, EuR 1981, S. 392–413.
Lackner, Karl/Kühl, Kristian (Hrsg.): Strafgesetzbuch. Kommentar, 28. Aufl. München 2014.
Lagodny, Otto: Strafrecht vor den Schranken der Grundrechte. Die Ermächtigung zum strafrechtlichen Vorwurf im Lichte der Grundrechtsdogmatik, Tübingen 1996.
Lampe, Ernst-Joachim: Die strafrechtliche Behandlung der sog. Computer-Kriminalität, GA 1975, S. 1–23.
Langbauer, Melanie: Das Strafrecht vor den Unionsgerichten, Berlin 2015.
Larenz, Karl: Methodenlehre der Rechtswissenschaft, Berlin u. a. 1969.
Lenaerts, Koen: Die EU-Grundrechtecharta: Anwendbarkeit und Auslegung, EuR 2012, S. 3–17.
Lenaerts, Koen/Gutiérrez-Fons/José Antonio: To Say What the Law of the EU Is. Methods of Interpretation and the European Court of Justice, EUI Working Paper AEL 2013, S. 3–48, abrufbar unter: http://cadmus.eui.eu/bitstream/handle/1814/28339/AEL_2013_09_DL.pdf?sequence=1 (Stand: 07.08.2017).
Lenz, Carl-Otto/Borchardt, Klaus-Dieter (Hrsg.): EU-Verträge Kommentar. EUV – AEUV – GRCh, 6. Aufl. Köln 2013 (zitiert: *Bearbeiter*, in: Lenz/Borchardt (Hrsg.)).
Lepsius, Oliver: Besitz und Sachherrschaft im öffentlichen Recht, Tübingen 2002.
Lesk, Michael: The New Front Line: Estonia under Cyberassault, IEEE Security & Privacy 2007, S. 76–79.
Ligeti, Katalin: Toward a Prosecutor for the European Union. Draft Rules of Procedure, Vol. 2, Oxford u. a. 2015.
Ligeti, Katalin: Toward a Prosecutor for the European Union. A Comparative Analysis, Vol. 1, Oxford u. a. 2013.
Ligeti, Katalin/Simonato, Michele: The European Public Prosecutor's Office: Towards a Truly European Prosecution Service?, NJECL 2013, S. 7–21.
Lisken, Hans: Verdachts- und ereignisunabhängige Personenkontrollen zur Bekämpfung der grenzüberschreitenden Kriminalität?, NVwZ 1998, S. 22–26.

Llera Suárez-Bárcena, Emilio de: La Policía Judicial y la seguridad ciudadana, Poder Judicial 1993, S. 107–124.

Lohse, Kai M.: The European Public Prosecutor: Issues of Conferral, Subsidiarity and Proportionality, in: Leendert Erkelens/Arjen Meij/Marta Pawlike (Hrsg.), The European Public Prosecutor's Office. An Extended Arm or a Two-Headed Dragon?, S. 165–182 (zitiert: *Lohse*, in: Erkelens/Meij/Pawlik (Hrsg.), The European Public Prosecutor's Office).

Long, Nadja: Towards a European Criminal Law Code?, European Institute of Public Administration Scope 2011, S. 49–52.

Luchtmann, Michiel J. J. P./Vervaele, John A. E.: European Agencies for Criminal Justice and Shared Enforcement (Eurojust and the European Public Prosecutor's Office), Utrecht Law Review 2014, S. 132–150.

Macke, Julia: UN-Sicherheitsrat und Strafrecht. Legitimation und Grenzen einer internationalen Strafgesetzgebung, Berlin 2010.

MacQuade, Samuel C.: Encyclopedia of Cybercrime, Westport 2009.

Marauhn, Thilo: Unionstreue, in: Rainer Schulze/Manfred Zuleeg/Stefan Kadelbach (Hrsg.), Europarecht. Handbuch für die deutsche Rechtspraxis, 3. Aufl. Baden-Baden 2015, S. 317–337 (zitiert: *Marauhn*, in: Schulze/Zuleeg/Kadelbach (Hrsg.), Europarecht).

Marberth-Kubicki, Annette: Computer- und Internetstrafrecht, 2. Aufl. München 2010.

Maunz, Theodor/Dürig, Günter (Hrsg.): Kommentar zum Grundgesetz, 53. Aufl. (76. EL, Stand: Dez. 2015) München 2009 (zitiert: *Bearbeiter*, in: Maunz/Dürig (Hrsg.)).

Mayer, Franz C.: Verfassungsgerichtsbarkeit, in: Armin von Bogdandy/Jürgen Bast (Hrsg.), Europäisches Verfassungsrecht: theoretische und dogmatische Grundzüge, 2. Aufl. Berlin u. a. 2009, S. 559–607 (zitiert: *Mayer*, in: von Bogdandy/Bast (Hrsg.), Europäisches Verfassungsrecht).

Mayer, Otto: Deutsches Verwaltungsrecht, Bd. 1, München 1895.

Mayer, Otto: Theorie des französischen Verwaltungsrechts, Bibliothek des öffentlichen Rechts, Goldbach 1886.

Mayer, Franz C./Wendel, Matthias: Die verfassungsrechtlichen Grundlagen des Europarechts, in: Armin Hatje/Peter-Christian Müller-Graff (Hrsg.), Enzyklopädie Europarecht. EnzEuR, Bd. 1: Europäisches Organisations- und Verfassungsrecht, Baden-Baden 2013, S. 163–258 (zitiert: *Mayer/Wendel*, in: Hatje/Müller-Graff (Hrsg.), EnzEuR).

Meier, Bernd-Dieter: Kriminologie und Internet: ein ungeklärtes Verhältnis, in: Susanne Beck/ders./Carsten Momsen (Hrsg.), Cybercrime und Cyberinvestigations. Neue Herausforderungen der Digitalisierung für Strafrecht, Strafprozessrecht und Kriminologie, Baden-Baden 2015, S. 93–118 (zitiert: *Meier*, in: Beck/ders./Momsen (Hrsg.), Cybercrime).

Meier, Bernd-Dieter: Sicherheit im Internet. Neue Herausforderungen für Kriminologie und Kriminalpolitik, MschrKrim 2012, S. 184–204.

Melander, Sakari: Ultima Ratio in European Criminal Law, EuCLR 2013, S. 45–64.

Meyer, Frank: Strafrechtsgenese in internationalen Organisationen. Eine Untersuchung der Strukturen und Legitimationsvoraussetzungen strafrechtlicher Normbildungsprozesse in Mehrebenensystemen, Baden-Baden 2012.

Meyer, Frank: Das Strafrecht im Raum der Freiheit, der Sicherheit und des Rechts, EuR 2011, S. 169–196.

Mitsch, Wolfgang: Vorbereitung und Strafrecht, JURA 2013, S. 696–704.

Mitsch, Wolfgang: Straflose Provokation strafbarer Taten, Lübeck 1986.

Mitsilegas, Vaslamis: The Third Wave of Third Pillar Law. Which Direction for EU Criminal Justive?, EL Rev 2009, S. 523–560.

Möllers, Christoph: German Federal Constitutional Court: Constitutional Ultra Vires Review of European Acts Only Under Exceptional Circumstances; Decision of 6 July 2010, 2 BvR 2661/06, Honeywell, EuConst 2011, S. 161–167.

Mühlen, Rainer A.H. von zur: Computer-Kriminalität. Gefahren und Abwehrmaßnahmen, Neuwied 1973.

Müller, Friedrich/Christensen, Ralph: Juristische Methodik, Bd. 2.: Europarecht, 3. Aufl. Berlin 2012.

Munoz, Nuria Pastor: Folgen der Bindung des mitgliedstaatlichen Strafgesetzgebers an die europäischen Regelungen und das Verhältnismäßigkeitsprinzip, eucrim 2008, S. 73–80.

Murray, Gillian: United against Cybercrime: the UNODC/ITU cybercrime capacity building initionative in: Stefano Manacorda (Hrsg.), Cibercriminality: Finding an Balance between Freedom and Security, 2012, S. 215–222 (zitiert: *Murray*, in: Manacorda (Hrsg.), Cibercriminality).

Nettesheim, Martin: Der Grundsatz der einheitlichen Wirksamkeit des Gemeinschaftsrechts, in: Albrecht Randelzhofer (Hrsg.), Gedächtnisschrift für Eberhard Grabitz, München 1995, S. 447–468 (zitiert: *Nettesheim*, in: GS-Grabitz (1995)).

Oberthür, Sebastian/Kelly, Clarie Roche: EU Leadership in International Climate Policy: Achievements and Challenges, The International Spectator 2008, S. 35–50.

OECD: Computer Viruses and Other Malicious Software: A Threat tot he Internet Economy, Paris 2009.

Oermann, Markus/Staben, Julian: Mittelbare Grundrechtseingriffe durch Abschreckung? Zur grundrechtlichen Bewertung polizeilicher „Online-Streifen" und „Online-Ermittlungen" in sozialen Netzwerken, Der Staat 2013, S. 630–661.

Oppermann, Thomas/Classen, Claus Dieter/Nettesheim, Martin (Hrsg.): Europarecht. Ein Studienbuch, 7. Aufl. München 2016 (zitiert: *Bearbeiter*, in: Oppermann/Classen/Nettesheim (Hrsg.), Europarecht).

Oppermann, Thomas: Den Musterknaben ins Bremserhäuschen! – Bundesverfassungsgericht und Lissabon-Vertrag, EuZW 2009, S. 437.

Paeffgen, Hans-Ullrich: Bürgerstrafrecht, Vorbeugungsrecht, Feindstrafrecht?, in: Martin Böse (Hrsg.), Grundlagen des Straf- und Strafverfahrensrechts. Festschrift für Knut Amelung zum 70. Geburtstag, Berlin 2009, S. 81–124 (zitiert: *Paeffgen*, in: FS Amelung (2009)).

Paramonova, Svetlana: Internationales Strafrecht im Cyberspace. Strafrechtliche Analyse der Rechtslage in Deutschland, Russland und den USA, Wiesbaden 2013.

Parker, Donn B.: Computer Crime. Criminal Justice Resource Manual: National Criminal Justice Information and Statistics Service, Law Enforcement Assistance Administration, U.S. Dept. of Justice, Washington, D.C. 1979, 2. Aufl. 1989, abrufbar unter: https://www.ncjrs.gov/pdffiles1/Digitization/118214NCJRS.pdf (Stand: 07.08.2017).

Pechstein, Matthias/Drechsler, Carola: Die Auslegung und Fortbildung des Primärrechts, in: Karl Riesenhuber (Hrsg.), Europäische Methodenlehre, 3. Aufl. Berlin u.a. 2015, S. 125–145 (zitiert: *Pechstein/Drechsler*, in: Riesenhuber (Hrsg.), Europäische Methodenlehre).

Peers, Steve: EU Criminal Law and the Treaty of Lisbon, EuLRev 2008, S. 507–529.

Pernice, Ingolf: Der Schutz nationaler Identität in der Europäischen Union, AöR 136 (2011), S. 185–221.

Pernice, Ingolf: La Rete Europea di Costituzionalià – Der Europäische Verfassungsverbund und die Netzwerktheorie, ZaöRV 70 (2010), S. 51–71.

Pernice, Ingolf: Europawissenschaft oder Staatsrechtslehre? – Eigenarten und Eigenständigkeit der Europarechtslehre, in: Helmuth Schulze-Fielitz (Hrsg.), Staatsrechtslehre als Wissenschaft, Die Verwaltung, Beiheft 7 (2007), S. 225–251 (zitiert: *Pernice*, in: Schulze-Fielitz (Hrsg.), Staatsrechtslehre als Wissenschaft).

Pernice, Ingolf: Theorie und Praxis des europäischen Verfassungsverbundes, in: Christian Calliess (Hrsg.), Verfassungswandel im europäischen Staaten- und Verfassungsverbund. Beiträge der Ersten Göttinger Gespräche zum Deutschen und Europäischen Verfassungsrecht vom 15. bis 17. Juni 2006, Tübingen 2007, S. 61–92 (zitiert: *Pernice*, in: Calliess (Hrsg.), Verfassungswandel im europäischen Staaten- und Verfassungsverbund).

Pernice, Ingolf: Das Verhältnis europäischer zu nationalen Gerichten im europäischen Verfassungsverbund, Berlin 2006.

Pernice, Ingolf: Der Europäische Verfassungsverbund auf dem Wege der Konsolidierung, JöR n. F. 48 (1999), S. 205–232.

Perron, Walter: Perspektiven der Europäischen Strafrechtsintegaration, in: Michael Hettinger (Hrsg.), Festschrift für Wilfried Küper zum 70. Geburtstag, Heidelberg 2007, S. 429–441 (zitiert: *Perron*, in: FS Küper (2007)).

Peterke, Sven/Noortman, Math: Transnationale kriminelle Organisationen im Völkerrecht: Mehr als Outlaws?, AdV 53 (2015), S. 1–34.

Piazena, Martin: Das Verabreden, Auffordern und Anleiten zur Begehung von Straftaten unter Nutzung der Kommunikationsmöglichkeiten des Internets, Berlin 2014.

Phelan, Diarmuid Rossa: Revolt or Revolution. The Constitutional Boundaries of the European Community, Dublin 1997.

Plender, Robert: The Interpretation of Community Acts by Reference to the Intentions of the Authors, Yearbook of European Law 1982, S. 57–105.

Polzin, Monika: Das Rangverhältnis von Verfassungs- und Unionsrecht nach der neuesten Rechtsprechung des BVerfG, JuS 2012, S. 1–6.

Pontell, Henry N./Geis, Gilbert/Brown, Gregory C.: Offshore Internet Gambling and the World Trade Organization. Is it Criminal Cehavior or a Commodity?, International Journal of Cyber Criminology 2007, S. 119–136.

Popp, Andreas: Strafbarer Bezug von kinder- und jugendpornographischen „Schriften“. Zeit für einen Paradigmenwechsel im Jugendschutzstrafrecht?, ZIS 2011, S. 193–204.

Popp, Andreas: § 202c StGB und der neue Typus des europäischen „Software-Delikts“, GA 2008, S. 375–393.

Prittwitz, Cornelius: Lissabon als Chance zur kriminalpolitischen Neubesinnung. Das Manifest zur Europäischen Kriminalpolitik, in: Kai Ambos (Hrsg.), Europäisches Strafrecht post-Lissabon, Göttingen 2011, S. 29–40 (zitiert: *Prittwitz*, in: Ambos (Hrsg.), Europäisches Strafrecht post-Lissabon).

Puschke, Jens: Grund und Grenzen des Gefährdungsstrafrechts am Beispiel der Vorbereitungsdelikte, in: Roland Hefendehl (Hrsg.), Grenzenlose Vorverlagerung des Strafrechts?, Berlin 2010, S. 9–40 (zitiert: *Puschke*, in Hefendehl (Hrsg.), Grenzenlose Vorverlagerung).

Quaglia, Lucia: The European Union and Global Financial Harmonisation, EUI Working Papers 2012, abrufbar unter: http://cadmus.eui.eu/bitstream/handle/1814/22234/SPS_2012_04.pdf (Stand: 07.08.2017).

Rath, Jürgen: Grundfälle zum Unrecht des Versuchs, JuS 1998, S. 1006–1111.

Raz, J.: The Rule of Law and its Virtue, Law Quarterly Review 93 (1977), S. 195–211.

Reinbacher, Tobias: Strafrecht im Mehrebenensystem. Modelle der Verteilung strafrechtsbezogener Kompetenzen, Baden-Baden 2014.

Reindl-Krauskopf, Susanne: Cyber-Kriminalität, ZaöRV 74 (2014), S. 563–574.

Rheinbay, Susanne: Die Errichtung einer Europäischen Staatsanwaltschaft, Berlin 2014.

Rissing, Ruth van/Tiedemann, Klaus/Laufhütte, Heinrich Wilhelm (Hrsg.): Leipziger Kommentar Strafgesetzbuch. StGB, 12. Aufl. 2007 ff. (zitiert: *Bearbeiter*, in: LK-StGB).

Robinson, Patrick: The Missing Crimes, in: Antonio Cassese/Paola Gaeta/John R.W.D. Jones (Hrsg.), The Rome Statute of the International Criminal Court. A Commentary, Vol. 1, S. 497–525 (zitiert: *Robinson*, in: The Rome Statute).

Rosbaud, Christian: Rome Statute of the International Criminal Court, Baden-Baden 2000.

Rosenau, Henning: Zur Europäisierung im Strafrecht, ZIS 2008, S. 9–19.

Roxin, Claus: Strafrecht. Allgemeiner Teil, Bd. 1.: Grundlagen. Der Aufbau der Verbrechenslehre, 4. Aufl. München 2006.

Ruggeri, Antonio: "Dialogue" Between European and National Courts, in the Pursuit of the Strongest Protection of Fundamental Rights (with Specific Regard to Criminal and Procedural Law), in: Stefano Ruggeri (Hrsg.), Human Rights in European Criminal Law. New Development in European Legislation and Case Law after the Lisbon Treaty, Heidelberg u. a. 2015, S. 9–30 (zitiert: *Ruggeri, A.,* in: Ruggeri, S. (Hrsg.), Human Rights in European Criminal Law).

Rüther, Werner: Phänomene der Internetdelinquenz. Ansätze, Probleme und Erkenntnisse zu ihrer gesellschaftlichen Definition und zu ihrer quantitativen Erfassung, in: Sandro Cimichella/André Kuhn/Marcel Alexander Niggli (Hrsg.), Neue Technologie und Kriminalität: Neue Kriminologie?, Zürich/Chur 2006, S. 85–117 (zitiert: *Rüther*, in: Cimichella u. a. (Hrsg.), Technologie und Kriminalität).

Sachs, Michael: Grundgesetz. Kommentar, 7. Aufl. München 2014 (zitiert: *Bearbeiter,* in: Sachs (Hrsg.), Grundgesetz).

Sauer, Heiko: „Solange" geht in Altersteilzeit – Der unbedingte Vorrang der Menschenwürde vor dem Unionsrecht, NJW 2016, S. 1134–1138.

Safferling, Christoph: Internationales Strafrecht, Heidelberg 2011.

Sandywell, Barry: On the Globalisation of Crime: the Internet and New Criminality, in: Yvonne Jewekes/Majid Yar (Hrsg.), Handbook of Internet Crime, Cullompton 2010, S. 38–66 (zitiert: *Sandywell*, in: Jewkes/Yar (Hrsg.), Handbook of Internet Crime).

Satzger, Helmut: Die Europäisierung des Strafrechts, Köln u. a. 2001.

Satzger, Helmut: Internationales und Europäisches Strafrecht. Strafanwendungsrecht, Europäisches Straf- und Strafverfahrensrecht, Völkerstrafrecht, 7. Aufl. Baden-Baden 2015.

Satzger, Helmut: Die potentielle Errichtung einer Europäischen Staatsanwaltschaft – Plädoyer für ein Komplementaritätsmodell, NStZ 2013, S. 206–213.

Savigny, Friedrich Carl von: System des heutigen römischen Rechts, Bd. 1, Frankfurt a. M. 2008.

Schaut, Andreas B.: Europäische Strafrechtsprinzipien. Ein Beitrag zur systematischen Fortentwicklung übergreifender Grundlagen, Baden-Baden 2012.

Schjølberg, Stein: The Third Pillar for Cyberspace – An International Court or Tribunal for Cyberspace, 10. Aufl. 2015; abrufbar unter: http://www.cybercrimelaw.net/documents/Draft_Treaty_text_on_International_Criminal_Tribunal_for_Cyberspace.pdf (Stand: 07.08.2017).

Schjølberg, Stein: The History of Global Harmonization on Cybercrime Legislation – The Road to Geneva, 2008, abrufbar unter: http://www.cybercrimelaw.net/documents/cybercrime_history.pdf (Stand: 07.08.2017).

Schjølberg, Stein/Hubbard, Amanda: Background Paper Harmonizing National and Legal Approaches on Cybercrime, ITU, Document CYB/04, 2005.

Schmidbauer, Wilhelm: Polizei zwischen Gefahrenabwehr und Strafverfolgung – Doppelfunktionale Maßnahmen der Polizei auf dem verfassungsrechtlichen Prüfstand, in: Gerrit

Manssen (Hrsg.), Nach geltendem Verfassungsrecht. Festschrift für Udo Steiner zum 70. Geburtstag, Stuttgart u. a. 2009, S. 734–757 (zitiert: *Schmidbauer*, in: FS Steiner (2009)).
Schmidt, Reiner: Die Liberalisierung der Daseinsvorsorge, Der Staat 42 (2003), S. 225–2247.
Schmidt, Rolf/Priebe, Klaus: Strafrecht. Besonderer Teil I. Straftaten gegen die Person und die Allgemeinheit, 14. Aufl. Grasberg 2015.
Schmitt, Michael N.: Tallinn Manual on the International Law Applicable to Cyber-Warfare, Cambridge 2013.
Schmölzer, Gabriele: Straftaten im Internet: eine materiell-rechtliche Betrachtung, ZStW 123 (2011), S. 709–736.
Schomburg, Wolfgang/Lagodny, Otto/Gleß, Sabine/Hackner, Thomas (Hrsg.): Internationale Rechtshilfe in Strafsachen, Beck'sche Kurz-Kommentare, 5. Aufl. München 2012 (zitiert: *Bearbeiter*, in Schomburg u. a. (Hrsg.), Rechtshilfe).
Schönke, Adolf/Schröder, Horst (Hrsg.): Strafgesetzbuch. Kommentar, 29. Aufl. München 2014 (zitiert: *Bearbeiter*, in: Schönke/Schröder (Hrsg.)).
Schramm, Edward: Auf dem Weg zur Europäischen Staatsanwaltschaft, JZ 2014, S. 749–758.
Schramm, Edward: Internationales Strafrecht. Strafanwendungsrecht, Völkerstrafrecht, europäisches Strafrecht, München 2011.
Schroeder, Werner: Die Auslegung des EU-Rechts, JuS 2004, S. 180–186.
Schuh, Daniel: Computerstrafrecht im Rechtsvergleich – Deutschland, Österreich und Schweiz, Berlin 2012.
Schultz, Alexander: Neue Strafbarkeiten und Probleme, DuD 2006, S. 778–784.
Schulze, Sven-Hendrick: Cyber-„War" – Testfall der Staatenverantwortlichkeit, Tübingen 2015.
Schulze, Tillmann: Bedingt abwehrbereit. Schutz kritischer Informations-Infrastrukturen in Deutschland und den USA, Wiesbaden 2006.
Schumann, Kay H.: Das 41. StrÄndG zur Bekämpfung der Computerkriminalität, NStZ 2007, S. 675–680.
Schünemann, Bernd: Spät kommt ihr, doch ihr kommt: Glosse eines Strafrechtlers zur Lissabon-Entscheidung des BVerfG, ZIS 2009, S. 393–396.
Schünemann, Bernd: Das Rechtsgüterschutzprinzip als Fluchtpunkt der verfassungsrechtlichen Grenzen der Straftatbestände und ihrer Interpretation, in: Roland Hefendehl/Andrew von Hirsch/Wolfgang Wohlers (Hrsg.), Die Rechtsgutstheorie. Legitimationsbasis des Strafrechts oder dogmatisches Glasperlenspiel?, Baden-Baden 2003, S. 133–154 (*Schünemann*, in: Hefendehl/von Hirsch/Wohlers (Hrsg.), Rechtsgutstheorie).
Schünemann, Bernd: Unzulänglichkeiten des Fahrlässigkeitsdelikts in der modernen Industriegesellschaft – Eine Bestandsaufnahme –, in: Eva Graul/Gerhard Wolf (Hrsg.), Gedächtnisschrift für Dieter Meurer, Berlin 2002, S. 37–64 (zitiert: *Schünemann*, in: GS Meurer (2002)).
Schwarze, Jürgen (Hrsg.): EU-Kommentar, 3. Aufl. Baden-Baden 2012 (zitiert: *Bearbeiter*, in: Schwarze (Hrsg.)).
Schwarze, Jürgen: Europäisches Verwaltungsrecht. Entstehung und Entwicklung im Rahmen der Europäischen Gemeinschaft, Bd. 2, 2. Aufl. Baden-Baden 2005.
Seger, Alexander: The Budapest Convention10 Years on: Lessons Learnt in: Stefano Manacorda (Hrsg.), Cibercriminality: Finding an Balance between Freedom and Security, 2012, S. 167–177 (zitiert: *Seger*, in: Manacorda (Hrsg.), Cibercriminality).
Shaw, Jo: European Union Legal Studies in Crisis? Towards a New Dynamic, OJLS 1996, Vol. 16, S. 231–253.

Sieben, Günter/von zur Mühlen, Rainer A. H.: Computerkriminalität – nicht Dichtung, sondern Wahrheit, DSWR 1972, S. 307–401.

Sieber, Ulrich/Vogel, Benjamin: Terrorismusfinanzierung: Prävention im Spannungsfeld von internationalen Vorgaben und nationalem Tatstrafrecht, Berlin 2015.

Sieber, Ulrich/Satzger, Helmut/von Heintschel-Heinegg, Bernd (Hrsg.): Europäisches Strafrecht, 2. Aufl. Baden-Baden 2014 (zitiert: *Bearbeiter*, in: Sieber/Satzger/von Heintschel-Heinegg (Hrsg.), Europäisches Strafrecht).

Sieber, Ulrich/Tropina, Tatiana/von zur Mühlen, Nicolas/Boran, Ian/Wright, Joss/Broadhurst, Roderic/Krüger, Kristin: Comprehensive Study on Cybercrime, 2013, abrufbar unter: http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf (Stand: 07.08.2017).

Sieber, Ulrich: Rechtliche Ordnung in einer globalen Welt, Initiative „MPG 2010+" der Max-Planck-Gesellschaft 2010, abrufbar unter: http://www.mpg.de/97975/HM01_Rechtliche_Ordnung-basetext.pdf (Stand: 07.08.2017).

Sieber, Ulrich: Die Zukunft des Europäischen Strafrechts – Ein neuer Ansatz zu den Zielen und Modellen des europäischen Strafrechtssystems –, ZStW 121 (2009), S. 1–67.

Sieber, Ulrich: Legitimation und Grenzen von Gefährdungsdelikten im Vorfeld von terroristischer Gewalt – Eine Analyse der Vorfeldtatbestände im „Entwurf eines Gesetzes zur Verfolgung der Vorbereitung von schweren staatsgefährdenden Gewalttaten –, NStZ 2009, S. 353–364.

Sieber, Ulrich: Sperrverpflichtungen gegen Kinderpronografie im Internet – Bewertung und Weiterentwicklung des Gesetzesentwurfs BT-Drucks. 16/12850 vom 5.5.2009, JZ 2009, S. 653–662.

Sieber, Ulrich: Mastering Complexity in the Global Cyberspace: The Harmonization of Computer-Related Criminal Law, in: Mireeille Delmas-Marty/Mark Pieth/Ulrich Sieber (Hrsg.), Les Chemins de l'Harmonisation pénale – Harmonising Criminal Law, Paris 2008, S. 127–202 (zitiert: *Sieber*, in: Delmas-Marty/Pieth/ders. (Hrsg.), Harmonising Criminal Law).

Sieber, Ulrich: Grenzen des Strafrechts – Grundlagen und Herausforderungen des neuen strafrechtlichen Forschungsprogramms am Max-Planck-Institut für ausländisches und internationales Strafrecht –, ZStW 119 (2007), S. 1–68.

Sieber, Ulrich: Einheitliches europäisches Strafgesetzbuch als Ziel der Strafrechtvergleichung?, in: Gunnar Duttge/Gerd Geilen/Lutz Meyer-Goßner/Günter Warda (Hrsg.), Gedächtnisschrift für Ellen Schlüchter, Köln u. a. 2002, S. 107–116 (zitiert: *Sieber*, in: GS Schlüchter (2002)).

Sieber, Ulrich: COMCRIME-Studie, 1998, abrufbar unter: http://www.edc.uoc.gr/~panas/PATRA/sieber.pdf (Stand: 07.08.2017).

Sieber, Ulrich: Computerkriminalität – Probleme hinter einem Schlagwort, DSWR 1974, S. 245–250.

Simma, Bruno u. a. (Hrsg.): The Charter of the United Nations. A Commentary, 3. Aufl. Oxford 2012 (zitiert: *Bearbeiter,* in: Simma u. a. (Hrsg.), The Charter of the United Nations).

Smend, Rudolf: Verfassung und Verfassungsrecht, München und Leipzig 1928.

Sofaer, Abraham D./Goodman, Seymour E./Cuéllar, Mariano-Florentino: The Transnational Dimension of Cyber Crime Terrorism, Stanford 2001.

Sonntag, Matthias: IT-Sicherheit kritischer Infrastrukturen. Von der Staatsaufgabe zur rechtlichen Ausgestaltung, München 2005.

Spannbrucker, Christian: Convention on Cybercrime (ETS 185) - Ein Vergleich mit dem deutschen Computerstrafrecht in materiell- und verfahrensrechtlicher Hinsicht, Regensburg 2005.

Spannowsky, Willy/Runkel, Peter/Goppel, Konrad (Hrsg.): Raumordnungsgesetz (ROG). Kommentar, München 2010 (zitiert: *Bearbeiter*, in: Spannowski/Runkel/Goppel (Hrsg.), Raumordnungsgesetz).

Spindler, Gerald/Schuster, Fabian (Hrsg.): Recht der elektronischen Medien, 3. Aufl. 2015 (zitiert: *Bearbeiter*, in: Spindler/Schuster (Hrsg.), Recht der elektronischen Medien).

Stegmann, Andrea: Organisierte Kriminalität. Feindstrafrechtliche Tendenzen in der Rechtsetzung zur Bekämpfung organisierter Kriminalität, Bern 2004.

Streinz, Rudolf (Hrsg.): EUV, AEUV. Vertrag über die Europäische Union und Vertrag über die Arbeitsweise der Europäischen Union, 2. Aufl. München 2012 (zitiert: *Bearbeiter*, in: Streinz (Hrsg.)).

Stuckenberg, Carl-Friedrich: Allgemeiner Teil eines europäischen Strafrechts, in: Martin Böse/Armin Hatje (Hrsg.), Enzyklopädie Europarecht. EnzEuR, Bd. 9: Europäisches Strafrecht. Mit polizeilicher Zusammenarbeit, Baden-Baden 2013, S. 379–412 (zitiert: *Stuckenberg*, in: Böse/Hatje (Hrsg.), EnzEuR).

Suárez-Bárcena, Emilio de Llera: La Policía Judicial y la seguridad ciudadana, Poder Judicial 1993, S. 107–124.

Suhr, Oliver: Die polizeiliche und justizielle Zusammenarbeit in Strafsachen nach dem „Lissabon"-Urteil des Bundesverfassungsgerichts, ZEuS 2009, S. 688–715.

Summers, Sarah: EU Criminal Law and the Regulation of Information and Communication Technolgy, Bergen Journal of Criminal Law & Criminal Justice, 2015, Vol. 2, S. 48–60.

Summers, Sarah/Schwarzenegger Christian/Ege, Gian/Young, Finlay: The Emergence of EU Criminal Law, Oxford u. a. 2014.

Suominen, Annika: The Past, Present and the Future of Eurojust, MJ 2008, S. 217–235.

Sybesma-Knol, Renera G.: The Status of Observers in the United Nations, Leiden 1981.

Theil, Stefan: What Red Lines, If Any, Do the Lisbon Judgments of European Constitutional Courts Draw for Future EU Integration?, GLJ 2014, S. 599–636.

Thym, Daniel: Flexible Integration. Garant oder Gefahr für die Einheit und die Legitimaion des Unionsrechts?, EuR Beiheft 2/2013, S. 23–49.

Tiedemann, Klaus: Wirtschaftsstrafrecht. Besonderer Teil mit wichtigen Rechtstexten, 3. Aufl. Köln u. a. 2011.

Tiedemann, Klaus (Hrsg.): Wirtschaftsstrafrecht in der Europäischen Union. Rechtsdogmatik, Rechtsvergleich, Rechtspolitik, Freiburger Symposium Wirtschaftsstrafrecht in der Europäischen Union, Köln 2002.

Tikk, Eneken/Kaska, Kadri/Vihul, Liis: International Cyber Incidents: Legal Considerations, Tallinn 2010.

Tikk, Eneken/Kaska, Kadri/Rünnimeri, Kristel/Kert, Mari/Talihärm, Anna-Maria/Vihul, Liis: Cyber Attacks Against Gerogia: Legal Lessons Identified, Tallinn 2008.

Timm, Frauke: Gesinnung und Strafrecht. Besinnung auf ein rechtsstaatliches Strafrecht, Berlin 2012.

Topa, Ilona: Where Do We Stand with Harmonization of Substantive Criminal Law in EU? Remarks on the Changes Introduced by the Lisbon Treaty, Silesian Journal of Legal Studies 2012, S. 89–99.

Tridimas, Takis: The General Princinples of EU Law, 2. Aufl. Oxford 2007.

Tropina, Tatiana: Cybersecruity, Cybercrime, Cyberwar? Terminology and Misconceptions, in: dies./Cormac Callanan, Self- and Co-regulation in Cybercime, Cybersecurity and Na-

tional Security, Heidelberg u. a. 2015, S. 4–10 (zitiert: *Tropina*, in: dies./Callanan (Hrsg.), Self- and Co-regulation in Cybercrime, Cybersecurity and National Security).

Turrini, Elliot/Ghosh, Sumit: A Pragmatic, Experiential Definition of Computer Crimes, in: dies. (Hrsg.), Cybercrime: A Multidisciplinary Analysis, Heidelberg u. a. 2010, S. 3–23 (zitiert: *Turrini/Ghosh*, in: dies. (Hrsg.), Cybercrimes).

UNODC: Cybercrime Repository 2016, abrufbar unter: https://www.unodc.org/cld/index-cybrepo.jspx (Stand: 07.08.2017).

UNODC: Crimes Related to Computer Networks – Background Paper for the Workshop on Crimes Related to the Computer Network, 10th UN Congress on the Prevention of Crime and the Treatment of Offenders, 2000, abrufbar unter: www.uncjin.org/Documents/congr10/10e.pdf (Stand: 07.08.2017).

Valerius, Brian: Zur Strafbarkeit virtueller Sit-ins im Internet, in: Eric Hilgendorf (Hrsg.), Dimensionen des IT-Rechts, Berlin 2008, S. 19–42 (zitiert: *Valerius*, in: Hilgendorf (Hrsg.), IT-Recht).

Valerius, Brian: Der Weg zu einem sicheren Internet?, K&R 2004, S. 513–518.

Vassilaki, Irni E.: Multimediale Kriminalität. Entstehung, Formen und rechtspolitische Fragen der Post-Computerkriminalität, CR 1997, S. 297–302.

Vedder, Christoph/Beutel, Jochen (Hrsg.): Europäischer Verfassungsvertrag. Handkommentar, Baden-Baden 2007 (zitiert: *Bearbeiter*, in: Vedder/Beutel (Hrsg.), Europäischer Verfassungsvertrag).

Velten, Petra: Europäisches Strafrecht, in: Erik Jayme/Heinz-Peter Mansel/Thomas Pfeiffer (Hrsg.), Jahrbuch für italienisches Recht, Heidelberg 2007, S. 173–194 (zitiert: *Velten*, in: Jayme/Mansel/Pfeiffer (Hrsg.), Jahrbuch für Italienisches Recht Bd. 20).

Vervaele, John A. E.: The Europeanisation of Criminal Law and the Criminal Law Dimension of European Integration, in: Paul Demaret (Hrsg.), European Legal Dynamics, Brüssel 2007, S. 277–298 (zitiert: *Vervaele*, in: Demaret u. a. (Hrsg.), European Legal Dynamics).

Vetter, Jan: Gesetzeslücken bei der Internetkriminalität, Konstanz 2003.

Villiger, Mark E.: Commentary on the 1969 Vienna Convention on the Law of Treaties, Leiden u. a. 2009.

Vitzthum, Wolfgang Graf (Hrsg.): Völkerrecht, 5. Aufl. Berlin u. a. 2010 (zitiert: *Bearbeiter*, in: Graf Vitzthum (Hrsg.), Völkerrecht).

Volger, Helmut (Hrsg.): Grundlagen und Strukturen der Vereinten Nationen, München u. a. 2007 (zitiert: *Bearbeiter*, in: Volger (Hrsg.), Grundlagen und Strukturen der Vereinten Nationen).

Vogel, Joachim: Begriff und Ziele der Harmonisierung, in: Martin Böse/Armin Hatje (Hrsg.), Enzyklopädie Europarecht. EnzEuR, Bd. 9: Europäisches Strafrecht. Mit polizeilicher Zusammenarbeit, Baden-Baden 2013, S. 269–286 (zitiert: *Vogel*, in: Böse/Hatje (Hrsg.), EnzEuR).

Vogel, Joachim: Strafgesetzgebungskompetenzen der Europäischen Union nach Art. 83, 86 und 325 AEUV, in: Kai Ambos (Hrsg.), Europäisches Strafrecht post-Lissabon, Göttingen 2011 (zitiert: *Vogel*, in: Ambos (Hrsg.), Europäisches Strafrecht post-Lissabon).

Vogel, Joachim: Die polizeiliche und justizielle Zusammenarbeit in Strafsachen, in: Burkhard Heß (Hrsg.), Wandel der Rechtsordnung, Tübingen 2003, S. 45–63 (zitiert: *Vogel*, in: Heß (Hrsg.), Wandel der Rechtsordnung).

Voßkuhle, Andreas: Der europäische Verfassungsgerichtsverbund, NVwZ 2010, S. 1–8.

Waechter, Kay: Die „Schleier-Fahndung“ als Instrument der indirekten Verhaltenssteuerung durch Abschreckung und Verunsicherung, DÖV 1999, S. 138–147.

Wagen, Wytske van der/Pieters, Wolter: From Cybercrime to Cyborg Crime: Botnets as Hybrid Criminal Actor-Networks, Brit. J. Criminol. 2015, S. 578–595.
Wall, David: Cybercrime: The Transformation of Crime in the Information Age, Cambridge u. a. 2011.
Walter, Christian: Cyber Security als Herausforderung für das Völkerrecht, JZ 2015, S. 685–693.
Walter, Tonio: Inwieweit erlaubt die Europäische Verfassung ein europäisches Strafgesetz?, ZStW 117 (2006), S. 912–933.
Watney, Murdoch M.: The Way Forward in Addressing Cybercrime Regulation on a Global Level, JITST, 2012, S. 61–67.
Weber, Manfred: Differenzierung nach Schutzbedürftigkeit des Versicherungsnehmers im Versicherungsrecht, in: Edgar Joussen/Rocco Jula/Sigurd Littbarksi (Hrsg.), Festschrift für Horst Baumann, S. 359–378 (zitiert: *Weber*, in: FS Baumann (1999)).
Wehrey, Frederic: Saudi Arabia's Anxious Autocrats, Journal of Democracy 2015, S. 71–85.
Weigend, Thomas: Der Entwurf einer Europäischen Verfassung und das Strafrecht, ZStW 116 (2004), S. 275–303.
Weigend, Thomas: Strafrecht durch internationale Vereinbarungen — Verlust an nationaler Strafrechtskultur?, ZStW 105 (1993), S. 774–802.
Weißer, Bettina: Strafrecht, in: Rainer Schulze/Manfred Zuleeg/Stefan Kadelbach (Hrsg.), Europarecht. Handbuch für die deutsche Rechtspraxis, 3. Aufl. Baden-Baden 2015, S. 2586–2652 (zitiert: *Weißer*, in: Schulze/Zuleeg/Kadelbach (Hrsg.), Europarecht).
Werle, Gerhard: Völkerstrafrecht, 3. Aufl. Tübingen 2012.
Wessels, Johannes/Beulke, Werner/Satzger, Helmut: Strafrecht Allgemeiner Teil. Die Straftat und ihr Aufbau, 45. Aufl. Heidelberg 2015.
Wieland, Joachim: Der EuGH im Spannungsverhältnis zwischen Rechtsanwendung und Rechtsgestaltung, NJW 2009, S. 1841–1845.
Wiener, Norbert: Kybernetik. Regelung und Nachrichtenübertragung in Lebewesen und Maschine, Reinbek bei Hamburg 1968.
Wischmeyer, Thomas: Nationale Identität und Verfassungsidentität. Schutzgehalte, Instrumente, Perspektiven, AöR 140 (2015), S. 415–460.
Wittzack, Maren: Das Recht der französischen Vollzugspolizeien. Eine vergleichende Untersuchung aus der Perspektive der Polizeirechtsordnung der Bundesrepublik Deutschland, Würzburg 2002.
Wolf, Sebastian: Die Modernisierung des deutschen Antikorruptionsstrafrechts durch internationale Vorgaben – Momentaufnahme und Ausblick, NJW 2006, S. 2735–2737.
Wolter, Jürgen (Hrsg.): Systematischer Kommentar zum Strafgesetzbuch, 8. Aufl. 2012 (zitiert: *Bearbeiter*, in: SK-StGB).
Yi, Won-Sang: Die Verhältnismäßigkeit im Cyberstrafrecht: Überprüfung des Strafrechtseingriffs im Cyberspace anhand des Verhältnismäßigkeitsgrundsatzes, Berlin 2010.
Zachariä, Heinrich Albert: Die Lehre vom Versuche der Verbrechen. Theil 1, Göttingen 1836.
Zeder, Fritz: Der Vorschlag zur Errichtung einer Europäischen Staatsanwaltschaft: große – kleine – keine Lösung?, StraFo 2014, S. 239–248.
Zimmermann, Frank: Strafgewaltkonflikte in der Europäischen Union. Ein Regelungsvorschlag zur Wahrung materieller und prozessualer strafrechtlicher Garantien sowie staatlicher Strafinteressen, Baden-Baden 2014.
Zimmermann, Frank: Die Auslegung künftiger EU-Strafrechtskompetenzen nach dem Lissabon-Urteil des Bundesverfassungsgerichts, JURA 2009, S. 844–851.

Zöller, Mark A.: Eurojust, EJN und Europäische Staatsanwaltschaft, in: Martin Böse/Armin Hatje (Hrsg.), Enzyklopädie Europarecht. EnzEuR, Bd. 9: Europäisches Strafrecht. Mit polizeilicher Zusammenarbeit, Baden-Baden 2013, S. 787–842 (zitiert: *Zöller*, in: Böse/Hatje (Hrsg.), EnzEuR).

Zöller, Mark A.: Neue unionsrechtliche Strafgesetzgebungskompetenzen nach dem Vertrag von Lissabon, in: Peter Baumeister/Wolfgang Roth/Josef Ruthig (Hrsg.), Staat, Verwaltung und Rechtsschutz. Festschrift für Wolf-Rüdiger Schenke zum 70. Geburtstag, Berlin 2011, S. 579–598 (zitiert: *Zöller*, in: FS Schenke (2011)).

Zöller, Mark A.: Willkommen in Absurdistan – Neue Straftatbestände zur Bekämpfung des Terrorismus, GA 2010, S. 607–621.

Zöller, Mark A.: Europäische Strafgesetzgebung, ZIS 2009, S. 340–349.

Zweigert, Konrad/Kötz, Hein: Einführung in die Rechtsvergleichung, 3. Aufl. Tübingen 1996.

Sachregister